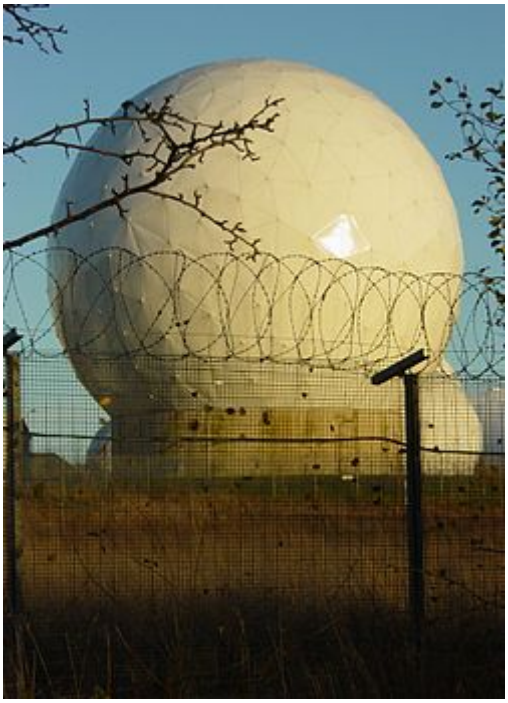
WIKIPEDIA

ECHELON

ECHELON, originally a secret government code name, is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the US with the aid of four other signatory nations to the UKUSA Security Agreement:[1] Australia, Canada, New Zealand and the United Kingdom, also known as the Five Eyes.[2][3][4]

The ECHELON program was 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, and it was formally established in 1971.[5][6]

By the end of the 20th century, the system referred to as "ECHELON" had evolved beyond its military and diplomatic origins to also become "...a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage).[7]



A radome at RAF Menwith Hill, a site with satellite uplink capabilities believed to be used by ECHELON.

RAF Menwith Hill, North Yorkshire, England

Contents

Name

The European Parliament's Temporary Committee on the ECHELON Interception System stated, "It seems likely, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that its name is in fact **ECHELON**, although this is a relatively minor detail".[7] The U.S. intelligence community uses many code names (*see*, for example, CIA cryptonym).

Former NSA employee Margaret Newsham claims that she worked on the configuration and installation of software that makes up the ECHELON system while employed at Lockheed Martin, from 1974 to 1984 in Sunnyvale, California, in the United States, and in Menwith Hill, England, in the UK.[8] At that time, according to Newsham, the code name ECHELON was NSA's term for the computer network itself. Lockheed called it *P415*. The software programs were called *SILKWORTH* and *SIRE*. A satellite named *VORTEX* intercepted communications. An image available on the internet of a fragment apparently torn from a job description shows Echelon listed along with several other code names.[9][10]

Misawa Air Base Security Operations Center (MSOC), Aomori Prefecture, Japan

Britain's *The Guardian* newspaper summarized the capabilities of the ECHELON system as follows:

> A global network of electronic spy stations that can eavesdrop on telephones, faxes and computers. It can even track bank accounts. This information is stored in Echelon computers, which can keep millions of records on individuals.
>
> Officially, however, Echelon doesn't exist.[11]

Reporting and disclosures

Public disclosures (1972–2000)

In 1972, former NSA analyst Perry Fellwock under pseudonym Winslow Peck, first blew the whistle on ECHELON to *Ramparts* in 1972,[12] where he gave commentary revealing a global network of listening posts and his experiences working there. Fellwock also included revelations such as the Israeli attack on USS *Liberty* was deliberate and known by both sides, the existence of nuclear weapons in Israel in 1972, the widespread involvement of CIA and NSA personnel in drugs and human smuggling, and CIA operatives leading Nationalist Chinese (Taiwan) commandos in burning villages inside PRC borders.[13]

In 1982, James Bamford, investigative journalist and author wrote *The Puzzle Palace*, an in-depth look inside the workings of the NSA, then a super-secret agency, and the massive eavesdropping operation under the codename "SHAMROCK". The NSA has used many codenames, and SHAMROCK was the code name used for ECHELON prior to 1975.[14][15]

In 1988, Margaret Newsham, a Lockheed employee under NSA contract, disclosed the ECHELON surveillance system to members of congress. Newsham told a member of the U.S. Congress that the telephone calls of Strom Thurmond, a Republican U.S. senator, were being collected by the NSA. Congressional investigators determined that "targeting of U.S. political figures would not occur by accident, but was designed into the system from the start."[16]

Also in 1988, an article titled "Somebody's Listening", written by investigative journalist Duncan Campbell in the *New Statesman*, described the signals intelligence gathering activities of a program code-named "ECHELON".[16] James Bamford describes the system as the software controlling the collection and distribution of civilian telecommunications traffic conveyed using communication satellites, with the collection being undertaken by ground stations located in the footprint of the downlink leg.[17]

A detailed description of ECHELON was provided by New Zealand journalist Nicky Hager in his 1996 book *Secret Power: New Zealand's Role in the International Spy Network*.[18] Two years later, Hager's book was cited by the European Parliament in a report titled "An Appraisal of the Technology of Political Control" (PE 168.184).[19]

In March 1999, for the first time in history, the Australian government admitted that news reports about the top secret UKUSA Agreement were true.[20] Martin Brady, the director of Australia's Defence Signals Directorate (DSD, now known as Australian Signals Directorate, or ASD) told the Australian broadcasting channel Nine Network that the DSD "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship."[21]

In 2000, James Woolsey, the former Director of the U.S. Central Intelligence Agency, confirmed that U.S. intelligence uses interception systems and keyword searches to monitor European businesses.[22]

Lawmakers in the United States feared that the ECHELON system could be used to monitor U.S. citizens.[23] According to *The New York Times*, the ECHELON system has been "shrouded in such secrecy that its very existence has been difficult to prove."[23] Critics said the ECHELON system emerged from the Cold War as a "Big Brother without a cause".[24]

European Parliament investigation (2000–2001)

The program's capabilities and political implications were investigated by a committee of the European Parliament during 2000 and 2001 with a report published in 2001.[7] In July 2000, the Temporary Committee on the ECHELON Interception System was established by the European parliament to investigate the surveillance network. It was chaired by the Portuguese politician Carlos Coelho, who was in charge of supervising investigations throughout 2000 and 2001.

The New Zealand journalist Nicky Hager, who testified before the European Parliament and provided specific details about the ECHELON surveillance system[25]

In May 2001, as the committee finalised its report on the ECHELON system, a delegation travelled to Washington, D.C. to attend meetings with U.S. officials from the following agencies and departments:

- U.S. Central Intelligence Agency (CIA)[26]
- U.S. Department of Commerce (DOC)[26]
- U.S. National Security Agency (NSA)[26]

All meetings were cancelled by the U.S. government and the committee was forced to end its trip prematurely.[26] According to a BBC correspondent in May 2001, "The US Government still refuses to admit that Echelon even exists."[5]

In July 2001, the Temporary Committee on the ECHELON Interception System released its final report.[27] On 5 September 2001, the European Parliament voted to accept the committee's report.[28]

The European Parliament stated in its report that the term ECHELON is used in a number of contexts, but that the evidence presented indicates that it was the name for a signals intelligence collection system. The report concludes that, on the basis of information presented, ECHELON was capable of interception and content inspection of telephone calls, fax, e-mail and other data traffic globally through the interception of communication bearers including satellite transmission, public switched telephone networks (which once carried most Internet traffic), and microwave links.[7]

Confirmation of ECHELON (2015)

Two internal NSA newsletters from January 2011 and July 2012, published as part of the Snowden-revelations by the website *The Intercept* on 3 August 2015, for the first time confirmed that NSA used the code word ECHELON and provided some details about the scope of the program: ECHELON was part of an umbrella program code named

FROSTING, which was established by the NSA in 1966 to collect and process data from communications satellites. FROSTING had two sub-programs:[29]

- TRANSIENT: for intercepting Soviet satellite transmissions
- ECHELON: for intercepting Intelsat satellite transmissions

Organization

The UKUSA intelligence community was assessed by the European Parliament (EP) in 2000 to include the signals intelligence agencies of each of the member states:

- the Government Communications Headquarters of the United Kingdom,
- the National Security Agency of the United States,
- the Communications Security Establishment of Canada,
- the Australian Signals Directorate of Australia, and
- the Government Communications Security Bureau of New Zealand.

The EP report concluded that it seemed likely that ECHELON is a method of sorting captured signal traffic, rather than a comprehensive analysis tool.[7]

UKUSA Community

Australia
Canada
New Zealand
United Kingdom
United States

Likely satellite intercept stations

In 2001, the EP report (p. 54 ff)[7] listed the following ground stations as likely to have, or to have had, a role in intercepting transmissions from telecommunications satellites:

- Hong Kong (since closed)
- Australian Defence Satellite Communications Station (Geraldton, Western Australia)
- RAF Menwith Hill (Yorkshire, U.K.) Map (https://maps.google.com/maps?f=q&geocode=&q=+54%C2%B0+0'31.29%22N+++1%C2%B041'22.17%22W&ie=UTF8&ll=54.009118,-1.689384&spn=0.003228,0.013561&t=k&z=17&om=1) (reportedly the largest Echelon facility)[30]
- Misawa Air Base (Japan) Map (https://maps.google.com/maps?ll=40.72051,141.326087)
- GCHQ Bude, formerly known as GCHQ CSO Morwenstow (Cornwall, U.K.) Map (https://maps.google.com/maps?f=q&source=s_q&geocode=&sspn=0.009846,0.019312&ie=UTF8&ll=50.885979,-4.553018&spn=0.008948,0.019312&t=h&z=16)
- Pine Gap (Northern Territory, Australia – close to Alice Springs) Map (https://maps.google.com/maps?f=q&geocode=&q=23.799S,+133.737E&ie=UTF8&ll=-23.798853,133.737066&spn=0.005026,0.013561&t=h&z=17)
- Sugar Grove (West Virginia, U.S.) Map (https://maps.google.com/maps?f=q&source=s_q&geocode=&sll=40.442767,-77.338257&sspn=2.763215,4.943848&ie=UTF8&ll=38.513906,-79.27964&spn=0.011098,0.019312&t=h&z=16) (since closed)
- Yakima Training Center (Washington, U.S.) Map (https://maps.google.com/maps?f=q&geocode=&q=46.68209++-120.356544&sll=46.681405,-120.356056&sspn=0.005186,0.004399&g=46.68209++-120.356544&ie=UTF8&t=k&ll=46.681795,-120.357381&spn=0.005185,0.006437&z=18&iwloc=addr) (since closed)
- GCSB Waihopai (New Zealand)[31]
- GCSB Tangimoana (New Zealand)[31]
- CFS Leitrim (Ontario, Canada)[32]
- Teufelsberg (Berlin, Germany) (closed 1992)[33] – Responsible for listening in to the Eastern Bloc.[34]

Other potentially related stations

The following stations are listed in the EP report (p. 57 ff) as ones whose roles "cannot be clearly established":

- Ayios Nikolaos (British Sovereign Base area of Dhekelia, Cyprus – U.K.)
- Gibraltar (U.K.)
- Diego Garcia (U.K.)

- Bad Aibling Station (Bad Aibling, Germany – U.S.)
  - relocated to Griesheim/Darmstadt in 2004.[35]
- Buckley Air Force Base (Aurora, Colorado)
- Fort Gordon (Georgia, U.S.)
- CFB Gander (Newfoundland & Labrador, Canada)
- Guam (Pacific Ocean, U.S.)
- Kunia Regional SIGINT Operations Center (Hawaii, U.S.)
- Lackland Air Force Base, Medina Annex (San Antonio, Texas)
- RAF Edzell (Scotland)
- RAF Boulmer (England)

List of intercept stations according to Edward Snowden's documents

Operated by the United States			
Country	**Location**	**Operator(s)**	**Codename**
Brazil	Brasília, Federal District	▪ CIA[36] ▪ NSA[36]	**SCS**
Germany	Bad Aibling, Munich	▪ BND[37] ▪ NSA[37]	**GARLICK**[38]
India	New Delhi	▪ CIA[39] ▪ NSA[39]	**SCS**
Japan	Misawa, Tōhoku region	▪ US Air Force[40] ▪ NSA[40]	**LADYLOVE**[41]
Thailand	Bangkok (?)	▪ CIA (?) ▪ NSA (?)	**LEMONWOOD**[42]
United Kingdom	Menwith Hill, Harrogate	▪ NSA[43]* GCHQ	**MOONPENNY**[42]
United States	Sugar Grove, West Virginia	▪ NSA[44]	**TIMBERLINE**[45]
	Yakima, Washington	▪ NSA[46]	**JACKKNIFE**[42]
	Sábana Seca, Puerto Rico	▪ NSA[47]	**CORALINE**[42]
Not operated by the United States (2nd party)			
Country	**Location**	**Contributor(s)**	**Codename**
Australia	Geraldton, WA	▪ ASD[40]	**STELLAR**[40]
	Darwin, NT	▪ ASD[40]	?[40]
New Zealand	Waihopai, Blenheim	▪ GCSB[40]	**IRONSAND**[40]
United Kingdom	Bude, Cornwall	▪ GCHQ[48] ▪ NSA[48]	**CARBOY**[45]
Cyprus	Ayios Nikolaos Station	▪ GCHQ[48] ▪ NSA[48]	**SOUNDER**[49]
Kenya	Nairobi	▪ GCHQ[40]	**SCAPEL**[42]
Oman		▪ GCHQ[40]	**SNICK**[42]

History and context

The ability to intercept communications depends on the medium used, be it radio, satellite, microwave, cellular or fiber-optic.[7] During World War II and through the 1950s, high-frequency ("short-wave") radio was widely used for military and diplomatic communication[50] and could be intercepted at great distances.[7] The rise of geostationary communications satellites in the 1960s presented new possibilities for intercepting international communications.

In 1964, plans for the establishment of the ECHELON network took off after dozens of countries agreed to establish the International Telecommunications Satellite Organisation (Intelsat), which would own and operate a global constellation of communications satellites.[20]

In 1966, the first Intelsat satellite was launched into orbit. From 1970 to 1971, the Government Communications Headquarters (GCHQ) of Britain began to operate a secret signal station at Morwenstow, near Bude in Cornwall, England. The station intercepted satellite communications over the Atlantic and Indian Oceans. Soon afterwards, the U.S. National Security Agency (NSA) built a second signal station at Yakima, near Seattle, for the interception of satellite communications over the Pacific Ocean.[20]

Equipment at the Yakima Research Station (YRS) in the early days of the ECHELON program

In 1981, GCHQ and the NSA started the construction of the first global wide area network (WAN). Soon after Australia, Canada, and New Zealand joined the ECHELON system.[20] The report to the European Parliament of 2001 states: "If UKUSA states operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax, and data traffic transmitted via such satellites."[7]

Teletype operators at the Yakima Research Station (YRS) in the early days of the ECHELON program

Most reports on ECHELON focus on satellite interception. Testimony before the European Parliament indicated that separate but similar UKUSA systems are in place to monitor communication through undersea cables, microwave transmissions, and other lines.[51] The report to the European Parliament points out that interception of private communications by foreign intelligence services is not necessarily limited to the U.S. or British foreign intelligence services.[7]

The role of satellites in point-to-point voice and data communications has largely been supplanted by fiber optics. In 2006, 99% of the world's long-distance voice and data traffic was carried over optical-fiber.[52] The proportion of international communications accounted for by satellite links is said to have decreased substantially to an amount between 0.4% and 5% in Central Europe.[7] Even in less-developed parts of the world, communications satellites are used largely for point-to-multipoint applications, such as video.[53] Thus, the majority of communications can no longer be intercepted by earth stations; they can only be collected by tapping cables and intercepting line-of-sight microwave signals, which is possible only to a limited extent.[7]

Concerns

British journalist Duncan Campbell and New Zealand journalist Nicky Hager asserted in the 1990s that the United States was exploiting ECHELON traffic for industrial espionage, rather than military and diplomatic purposes.[51] Examples alleged by the journalists include the gear-less wind turbine technology designed by the German firm Enercon[7][54] and the speech technology developed by the Belgian firm Lernout & Hauspie.[55]

In 2001, the Temporary Committee on the ECHELON Interception System recommended to the European Parliament that citizens of member states routinely use cryptography in their communications to protect their privacy, because economic espionage with ECHELON has been conducted by the U.S. intelligence agencies.[7]

American author James Bamford provides an alternative view, highlighting that legislation prohibits the use of intercepted communications for commercial purposes, although he does not elaborate on how intercepted communications are used as part of an all-source intelligence process.

In its report, the committee of the European Parliament stated categorically that the Echelon network was being used to intercept not only military communications, but also private and business ones. In its epigraph to the report, the parliamentary committee quoted Juvenal, "*Sed quis custodiet ipsos custodes.*" ("But who will watch the watchers").[7] James Bamford, in *The Guardian* in May 2001, warned that if Echelon were to continue unchecked, it could become a "cyber secret police, without courts, juries, or the right to a defence".[56]

Alleged examples of espionage conducted by the members of the "Five Eyes" include:

- On behalf of the British Prime Minister Margaret Thatcher, the Communications Security Establishment spied on two British cabinet ministers in 1983.[57]
- The U.S. National Security Agency spied on and intercepted the phone calls of Diana, Princess of Wales right until she died in a Paris car crash with Dodi Fayed in 1997. The NSA currently holds 1,056 pages of classified information about Princess Diana, which has been classified as top secret "because their disclosure could reasonably be expected to cause exceptionally grave damage to the national security ... the damage would be caused not by the information about Diana, but because the documents would disclose 'sources and methods' of U.S. intelligence gathering".[58] An official insisted that "the references to Diana in intercepted conversations were 'incidental'," and she was never a 'target' of the NSA eavesdropping.[58]
- U.K. agents monitored the conversations of the 7th Secretary-General of the United Nations Kofi Annan.[59][60]
- U.S. agents gathered "detailed biometric information" on the 8th Secretary-General of the United Nations, Ban Ki-Moon.[61][62]
- In the early 1990s, the U.S. National Security Agency intercepted the communications between the European aerospace company Airbus and the Saudi Arabian national airline. In 1994, Airbus lost a $6 billion contract with Saudi Arabia after the NSA, acting as a whistleblower, reported that Airbus officials had been bribing Saudi officials to secure the contract.[63] As a result, the American aerospace company McDonnell Douglas (now part of Boeing) won the multibillion-dollar contract instead of Airbus.[64]
- The American defense contractor Raytheon won a US$1.3 billion contract with the Government of Brazil to monitor the Amazon rainforest after the U.S. Central Intelligence Agency (CIA), acting as a whistleblower, reported that Raytheon's French competitor Thomson-Alcatel had been paying bribes to get the contract.[65]
- In order to boost America's position in trade negotiations with the then Japanese Trade Minister Ryutaro Hashimoto, in 1995 the CIA eavesdropped on the conversations between Japanese bureaucrats and executives of car manufacturers Toyota and Nissan.[66]

Workings

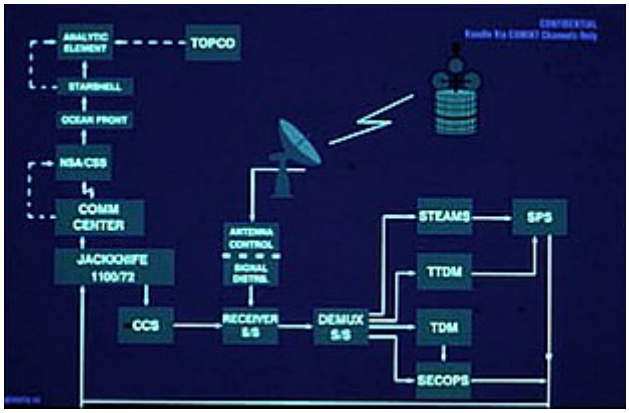
The first American satellite ground station for the ECHELON collection program was built in 1971 at a military firing and training center near Yakima, Washington. The facility, which was codenamed JACKKNIFE, was an investment of ca. 21.3 million dollars and had around 90 people. Satellite traffic was intercepted by a 30-meter single dish antenna. The station became fully operational on 4 October 1974. It was connected with NSA headquarters at Fort Meade by a 75-baud secure Teletype orderwire channel.[29]

In 1999 the Australian Senate Joint Standing Committee on Treaties was told by Professor Desmond Ball that the Pine Gap facility was used as a ground station for a satellite-based interception network. The satellites were said to be large radio dishes between 20 and 100 meters in diameter in geostationary orbits. The original purpose of the network was

to monitor the telemetry from 1970s Soviet weapons, air defence and other radars' capabilities, satellites' ground stations' transmissions and ground-based microwave communications.[68]

Examples of industrial espionage

In 1999, Enercon, a German company and leading manufacturer of wind energy equipment, developed a breakthrough generator for wind turbines. After applying for a US patent, it had learned that Kenetech, an American rival, had submitted an almost identical patent application shortly before. By the statement of a former NSA employee, it was later discovered that the NSA had secretly intercepted and monitored Enercon's data communications and conference calls and passed information regarding the new generator to Kenetech.[69] As German intelligence services are forbidden from engaging in industrial or economic espionage, German companies are frequently complaining that this leaves them defenceless against industrial espionage from the United States. According to Wolfgang Hoffmann, a former manager at Bayer, German intelligence services are aware which companies are being targeted by US intelligence agencies, but refuse to inform the companies involved.[70]



System diagram of the ECHELON satellite intercept station of the NSA at the Yakima Research Station (YRS) [67]
TOPCO = Terminal Operations Control
CCS = Computer Control Subsystem
STEAMS = System Test, Evaluation, Analysis, and Monitoring Subsystem
SPS = Signal Processing Subsystem
TTDM = Teletype Demodulator

In popular culture

The television series *Alias* made recurring references to ECHELON throughout its run.

The antagonist of the anime series *Digimon Tamers*, D-Reaper, was created by ECHELON.

Echelon Conspiracy, inspired by the surveillance system ECHELON, is a 2009 action thriller film directed by Greg Marcks. It tells the story of Max Peterson (Shane West), an American computer specialist who attempts to uncover a secret plot to turn the world into a global police state. After being chased down by NSA agent Raymond Burke (Martin Sheen), Peterson decides to flee to Moscow.

The video game series *Tom Clancy's Splinter Cell* also draws inspiration from this. The series features the protagonist, Sam Fisher, a trained operative belonging to a fictional branch of the National Security Agency called Third Echelon (later, in *Splinter Cell: Blacklist*, the unit is replaced by the Fourth Echelon).

The 2007 film *The Bourne Ultimatum* makes several references to ECHELON. A CIA listening station in London is alerted when ECHELON detects the keyword "Blackbriar" in a cell phone conversation between a journalist and his editor.[71] Later in the film, CIA Deputy Director Pamela Landy requests an "ECHELON package" on the main character, Jason Bourne.

In the 2000 computer game *Deus Ex*, the signals intelligence supercomputers Daedalus and Icarus (later Helios) are referred to as Echelon IV.

The New Zealand wine label Spy Valley is named after the nearby Waihopai Valley facility

The sci-fi crime thriller, *Person of Interest*, a television show which aired from 2011 to 2016 on the CBS network, had a data-collecting supercomputer as its central narrative.

In *Steins;Gate* SERN monitors if someone sends a D-mail through ECHELON.

The ABC series "Pine Gap" is based on the communications control network.

See also

- 2013 mass surveillance disclosures
- ADVISE
- Frenchelon
- List of government surveillance projects
- Mass surveillance
- Onyx (interception system), the Swiss "Echelon"
- Operation Ivy Bells

Bibliography

- Aldrich, Richard J.; *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*, HarperCollins, July 2010. ISBN 978-0-00-727847-3
- Bamford, James; *The Puzzle Palace*, Penguin, ISBN 0-14-006748-5; 1983
- Bamford, James; *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Doubleday, ISBN 0-385-52132-4; 2008
- Hager, Nicky; *Secret Power: New Zealand's Role in the International Spy Network*; Craig Potton Publishing, Nelson, NZ; ISBN 0-908802-35-8; 1996
- Keefe, Patrick Radden *Chatter: Dispatches from the Secret World of Global Eavesdropping*; Random House Publishing, New York, NY; ISBN 1-4000-6034-6; 2005
- Keefe, Patrick (2006). *Chatter : uncovering the echelon surveillance network and the secret world of global eavesdropping*. New York: Random House Trade Paperbacks. ISBN 978-0-8129-6827-9.
- Lawner, Kevin J.; Post-Sept. 11th International Surveillance Activity - A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe (http://digitalcommons.pace.edu/pilr/vol14/iss2/7), 14 *Pace Int'l L. Rev.* 435 (2002)

Notes and references

1. Given the 5 dialects that use the terms, UKUSA can be pronounced from "You-Q-SA" to "Oo-Coo-SA", AUSCANNZUKUS can be pronounced from "Oz-Can-Zuke-Us" to "Orse-Can-Zoo-Cuss".
   > From Talk:UKUSA Agreement: "Per documents officially released by both the Government Communications Headquarters and the National Security Agency, this agreement is referred to as the UKUSA Agreement. This name is subsequently used by media sources reporting on the story, as written in new references used for the article. The NSA press release provides a pronunciation guide, indicating that "UKUSA" should not be read as two separate entities."(The National Archives)" (https://web.archive.org/web/20130502100834/http://www.nationalarchives.gov.uk/news/471.htm). Archived from the original on 2 May 2013. Retrieved 2012-10-10. (National Security Agency) (http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml)"
2. "UK 'biggest spy' among the Five Eyes" (http://www.news.com.au/technology/uk-spying-more-extensive-than-in-us/story-e6frfro0-1226667900434). News Corp Australia. 22 June 2013. Retrieved 19 October 2013.
3. Google books – Echelon (https://books.google.com/books?id=1x6Akzkxv5IC&printsec=frontcover&source=gbs_summary_r&cad=0) by John O'Neill
4. "AUSCANNZUKUS Information Portal" (https://web.archive.org/web/20120220104120/http://auscannzukus.net/). auscannzukus.net. Archived from the original (http://auscannzukus.net/) on 2012-02-20. Retrieved 1 February 2010.
5. "Q&A: What you need to know about Echelon" (http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm). BBC. 29 May 2001.
6. Nabbali, Talitha; Perry, Mark (March 2004). "Going for the throat" (http://www.sciencedirect.com/science/article/pii/S0267364904000184). *Computer Law & Security Review*. **20** (2): 84–97. doi:10.1016/S0267-3649(04)00018-4 (https://doi.org/10.1016%2FS0267-3649%2804%2900018-4). "It wasn't until 1971 that the UKUSA allies began ECHELON"

7. Schmid, Gerhard (11 July 2001). "On the existence of a global system for the interception of private and commercial communications (ECHELON interception system), (2001/2098(INI))" (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN) (pdf – 194 pages). European Parliament: Temporary Committee on the ECHELON Interception System. Retrieved 5 January 2013.
8. Elkjær, Bo; Kenan Seeberg (17 November 1999). "ECHELON Was My Baby" (http://cryptome.org/echelon-baby.htm). *Ekstra Bladet*. Retrieved 17 May 2006. "Unfortunately, I can't tell you all my duties. I am still bound by professional secrecy, and I would hate to go to prison or get involved in any trouble, if you know what I mean. In general, I can tell you that I was responsible for compiling the various systems and programs, configuring the whole thing and making it operational on mainframes"; "Margaret Newsham worked for the NSA through her employment at Ford and Lockheed from 1974 to 1984. In 1977 and 1978 Newsham was stationed at the largest listening post in the world at Menwith Hill, England ... Ekstra Bladet has Margaret Newsham's stationing orders from the US Department of Defense. She possessed the high security classification TOP SECRET CRYPTO."
9. Goodwins, Rupert (29 June 2000). "Echelon: How it works" (http://www.zdnet.com/echelon-how-it-works-3002079849/). ZDNet. Retrieved 28 January 2014.
10. =Campbell, Duncan (25 July 2000). "Inside Echelon" (http://www.zdnet.com/echelon-how-it-works-3002079849/). Heise Online. Retrieved 28 January 2014.
11. Perrone, Jane (29 May 2001). "The Echelon spy network" (https://www.theguardian.com/world/2001/may/29/qanda.janeperrone). *The Guardian*. Retrieved 28 January 2014.
12. David Horowitz (August 1972). "U.S. Electronic Espionage: A Memoir". *Ramparts*. **11** (2): 35–50.
13. "Ramparts interview" (http://cryptome.org/jya/nsa-elint.htm). Cryptome archive. 1988. Retrieved April 21, 2017.
14. Bamford, James (1982). *The Puzzle Palace: A Report on America's Most Secret Agency*. Houghton Mifflin. ISBN 0-14-006748-5.
15. "Puzzle Palace excepts" (http://cryptome.org/jya/echelon-dc.htm). Cryptome archive. Retrieved April 21, 2017.
16. Campbell, Duncan (12 August 1988). "Somebody's Listening" (http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf) (PDF). *New Statesman*. Retrieved 27 November 2013.
17. Bamford, James (2002). *Body of Secrets*. Anchor. ISBN 0-385-49908-6.
18. Duncan Campbell (1 June 2001). "Echelon Chronology" (http://www.heise.de/tp/artikel/7/7795/1.html). Heise Online. Retrieved 19 December 2013.
19. Wright, Steve (6 January 1998). "An Appraisal of Technologies of Political Control" (http://www.europarl.europa.eu/pdf/jadis/2013_12/8.PE4_AP_PV!LIBE.1994_LIBE-199801260050EN.pdf) (PDF). European Parliament. Retrieved 28 January 2014.
20. Duncan Campbell. "Echelon: World under watch, an introduction" (http://www.zdnet.com/echelon-world-under-watch-an-introduction-3002079845/). ZDNet. Retrieved 19 December 2013.
21. Duncan Campbell and Mark Honigsbaum (23 May 1999). "Britain and US spy on world" (https://www.theguardian.com/uk/1999/may/23/duncancampbell.markhonigsbaum). *The Observer*. Retrieved 19 December 2013.
22. R. James Woolsey (17 March 2000). "Why We Spy on Our Allies" (https://www.wsj.com/articles/SB95326824311657269). *The Wall Street Journal*.
23. Niall McKay (27 May 1999). "Lawmakers Raise Questions About International Spy Network" (https://www.nytimes.com/library/tech/99/05/cyber/articles/27network.html). *The New York Times*. Retrieved 19 December 2013.
24. Suzanne Daley (24 February 2000). I "An Electronic Spy Scare Is Alarming Europe" (https://www.nytimes.com/library/tech/00/02/biztech/articles/24spy.htm) Check |`url=` value (help). *The New York Times*. Retrieved 19 December 2013.
25. Kieren McCarthy (14 September 2001). "This is how we know Echelon exists" (https://www.theregister.co.uk/2001/09/14/this_is_how_we_know/). *The Register*. Retrieved 19 December 2013.
26. Roxburgh, Angus (11 May 2001). "EU investigators 'snubbed' in US" (http://news.bbc.co.uk/2/hi/europe/1325186.stm). BBC. Retrieved 28 January 2014.
27. "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))" (http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN). European Parliament. 11 July 2001. Retrieved 10 September 2013.

28. "Report: Echelon exists, should be guarded against" (http://usatoday30.usatoday.com/tech/news/2001-09-05-echelon.htm). *USA Today*. Associated Press. 5 September 2001. Retrieved 7 February 2014.
29. The Northwest Passage, Yakima Research Station (YRS) newsletter: Volume 2, Issue 1, January 2011 (http://www.documentcloud.org/documents/2189960-nwp-nsa.html) & Volume 3, Issue 7, July 2012 (http://www.documentcloud.org/documents/2189961-nwp2-nsa.html).
30. Le Monde Diplomatique (http://mondediplo.com/2010/09/04israelbase), September 2010
31. Eames, David (19 March 2010). "Waihopai a key link in global intelligence network" (http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10632956). *The New Zealand Herald*. Retrieved 28 January 2014. "Both Waihopai and the Tangimoana radio listening post near Palmerston North have been identified as key players in the United States-led Echelon spy programme."
32. Stupak, edited by David S. Greisler, Ronald J. (2007). *Handbook of technology management in public administration*. CRC/Taylor & Francis. p. 592. ISBN 1420017012.
33. "Teufelsberg mirrors Berlin's dramatic history" (http://www.dw.de/teufelsberg-mirrors-berlins-dramatic-history/a-17074597). Deutsche Welle. Retrieved 28 January 2014. "More than 1,000 people are said to have worked here around the clock, every day of the year. They were part of the global ECHELON surveillance network."
34. Beddow, Rachel. "Teufelsberg, Berlin's Undisputed King Of Ghostowns, Set For Redevelopment" (https://www.npr.org/blogs/nprberlinblog/2012/04/16/150730955/teufelsberg-berlins-undisputed-king-of-ghostowns-set-for-redevelopment). NPR. Retrieved 28 January 2014. "The Teufelsberg mission is still shrouded in secrecy, but it's generally agreed that the station was part of the ECHELON network that listened in to the Eastern Bloc."
35. According to a statement by Terence Dudlee, the speaker of the US Navy in London, in an interview to the German HR (Hessischer Rundfunk)
"US-Armee lauscht von Darmstadt aus" (https://archive.is/20070630004752/http://www6.hr-online.de/website/rubriken/nachrichten/index.jsp?rubrik=5710&key=standard_document_2406678). Archived from the original (http://www6.hr-online.de/website/rubriken/nachrichten/index.jsp?rubrik=5710&key=standard_document_2406678) on 30 June 2007. Retrieved 19 August 2016. (German), *hr online*, 1 October 2004
36. Roberto Kaz e José Casado. "Capitais de 4 países também abrigaram escritório da NSA e CIA" (http://oglobo.globo.com/mundo/capitais-de-4-paises-tambem-abrigaram-escritorio-da-nsa-cia-8966597). *O Globo* (in Portuguese). Retrieved 31 January 2014.
37. Hubert Gude, Laura Poitras and Marcel Rosenbach. "German Intelligence Sends Massive Amounts of Data to the NSA" (http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html). *Der Spiegel*. Retrieved 31 January 2014.
38. "Cover Story: How the NSA Targets Germany and Europe" (http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-2.html). *Der Spiegel*. Retrieved 31 January 2014.
39. "US spy centre in India too" (https://web.archive.org/web/20140202182811/http://www.deccanchronicle.com/131030/news-current-affairs/article/us%E2%80%88spy-centre-india-too). *Deccan Chronicle*. 30 October 2013. Archived from the original (http://www.deccanchronicle.com/131030/news-current-affairs/article/us%E2%80%88spy-centre-india-too) on 2 February 2014. Retrieved 31 January 2014.
40. Dorling, Philip. "Singapore, South Korea revealed as Five Eyes spying partners" (http://www.smh.com.au/technology/technology-news/singapore-south-korea-revealed-as-five-eyes-spying-partners-20131124-2y433.html). *The Sydney Morning Herald*. Retrieved 30 January 2014.
41. "Document 12. "Activation of Echelon Units," from History of the Air Intelligence Agency, 1 January - 31 December 1994, Volume I (San Antonio, TX: AIA, 1995)". George Washington University. "The second extract notes that AIA's participation in a classified activity "had been limited to LADYLOVE operations at Misawa AB [Air Base], Japan."" Missing or empty |url= (help); |access-date= requires |url= (help)
42. "Eyes Wide Open" (https://web.archive.org/web/20140106052052/https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf) (PDF). Privacy International. p. 11. Archived from the original (https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf) (PDF) on 6 January 2014. Retrieved 31 January 2014.
43. Norton-Taylor, Richard (1 March 2012). "Menwith Hill eavesdropping base undergoes massive expansion" (https://www.theguardian.com/world/2012/mar/01/menwith-hill-eavesdropping-base-expansion). *The Guardian*. Retrieved 31 January 2014.
44. Steelhammer, Rick (4 January 2014). "In W.Va., mountains of NSA secrecy" (http://www.wvgazette.com/News/201401040095). *The Charleston Gazette*. Retrieved 31 January 2014.

45. Laura Poitras, Marcel Rosenbach and Holger Stark. "Friendly Fire: How GCHQ Monitors Germany, Israel and the EU" (http://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135-2.html). *Der Spiegel*. Retrieved 31 January 2014.
46. Troianello, Craig (4 April 2013). "NSA to close Yakima Training Center facility" (https://web.archive.org/web/20140219144524/http://seattletimes.com/html/localnews/2020713369_listeningpostxml.html). *The Seattle Times*. Archived from the original (http://seattletimes.com/html/localnews/2020713369_listeningpostxml.html) on 19 February 2014. Retrieved 31 January 2014.
47. Roberto Kaz and José Casado. "Capitais de 4 países também abrigaram escritório da NSA e CIA" (http://oglobo.globo.com/mundo/capitais-de-4-paises-tambem-abrigaram-escritorio-da-nsa-cia-8966597). *O Globo* (in Portuguese). Retrieved 31 January 2014.
48. Nick Hopkins and Julian Borger (1 August 2013). "Exclusive: NSA pays £100m in secret funding for GCHQ" (https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden). *The Guardian*. Retrieved 31 January 2014.
49. Squires, Nick (5 November 2013). "British military base in Cyprus 'used to spy on Middle East'" (https://www.telegraph.co.uk/news/worldnews/europe/cyprus/10427890/British-military-base-in-Cyprus-used-to-spy-on-Middle-East.html). *The Daily Telegraph*. London. Retrieved 31 January 2014.
50. *The Codebreakers*, Ch. 10, 11
51. For example: "Nicky Hager Appearance before the Euro ean Parliament ECHELON Committee" (http://cryptome.org/echelon-nh.htm). April 2001. Retrieved 2 July 2006.
52. "NSA eavesdropping: How it might work" (http://news.cnet.com/NSA+eavesdropping+How+it+might+work/2100-1028_3-6035910.html). *CNET News.com*. Retrieved 27 August 2006.
53. "Commercial Geostationary Satellite Transponder Markets for Latin America : Market Research Report" (http://www.marketresearch.com/map/prod/1117944.html). Retrieved 27 August 2006.
54. Die Zeit: 40/1999 "*Verrat unter Freunden*" ("Treachery among friends", German), available at "Zeit.de" (https://web.archive.org/web/20081009044725/http://www.zeit.de/1999/40/199940.nsa_2_.xml). Archived from the original on 9 October 2008. Retrieved 2007-08-19.
55. "Amerikanen maakten met Echelon L&H kapot" (http://www.daanspeak.com/Hypocratie09.html). daanspeak.com. 30 March 2002. Archived (https://www.webcitation.org/66Jmuc30R?url=http://www.daanspeak.com/Hypocratie09.html) from the original on 21 March 2012. Retrieved 28 March 2008. (Google's translation of the article into English (https://translate.google.com/translate?hl=en&sl=nl&u=http://www.daanspeak.com/Hypocratie09.html&sa=X&oi=translate&resnum=1&ct=result)).
56. Bustillos, Maria (9 June 2013). "Our reflection in the N.S.A.'s PRISM" (http://www.newyorker.com/online/blogs/elements/2013/06/a-reflection-in-the-nsas-prism.html). *The New Yorker*. Retrieved: 2013-10-12.
57. "Thatcher 'spied on ministers'" (http://news.bbc.co.uk/2/hi/uk_news/politics/655996.stm). BBC. 25 February 2000.
58. Vernon Loeb (12 December 1998). "NSA Admits to Spying on Princess Diana" (https://www.washingtonpost.com/wp-srv/national/daily/dec98/diana12.htm). *The Washington Post*.
59. "UK 'spied on UN's Kofi Annan'" (http://news.bbc.co.uk/2/hi/uk_news/politics/3488548.stm). BBC. 26 February 2004. Retrieved 21 September 2013.
60. PATRICK E. TYLER (26 February 2004). "Ex-Minister Says British Spies Bugged Kofi Annan's Office" (https://www.nytimes.com/2004/02/26/international/europe/26CND-BRIT.html). *The New York Times*. Retrieved 21 September 2013.
61. "US diplomats spied on UN leadership" (https://www.theguardian.com/world/2010/nov/28/us-embassy-cables-spying-un). *The Guardian*. Retrieved 27 August 2013.
62. Marcel Rosenbach and Holger Stark. "Diplomats or Spooks? How US Diplomats Were Told to Spy on UN and Ban Ki-Moon" (http://www.spiegel.de/international/world/diplomats-or-spooks-how-us-diplomats-were-told-to-spy-on-un-and-ban-ki-moon-a-731747.html). *Der Spiegel*. Retrieved 27 August 2013.
63. "Echelon: Big brother without a cause" (http://news.bbc.co.uk/1/hi/world/europe/820758.stm). BBC News. 6 July 2000. Retrieved 27 August 2006.
64. "Airbus's secret past" (http://www.economist.com/node/1842124). *The Economist*. 14 June 2003. Retrieved 15 October 2013.
65. "Big Surveillance Project For the Amazon Jungle Teeters Over Scandals" (http://www.csmonitor.com/1996/0125/25071.html/%28page%29/2). *The Christian Science Monitor*. Retrieved 15 October 2013.

66. David E. Sanger and Tim Weiner (15 October 1995). "Emerging Role For the C.I.A.: Economic Spy" (https://www.nytimes.com/1995/10/15/world/emerging-role-for-the-cia-economic-spy.html). *The New York Times*. Retrieved 15 October 2013.
67. The Northwest Passage, Yakima Research Station (YRS) newsletter: Volume 2, Issue 1, January 2011 (http://www.documentcloud.org/documents/2189960-nwp-nsa.html).
68. "Pine Gap" (https://web.archive.org/web/20110608040058/http://www.aph.gov.au/hansard/joint/commttee/j2408.pdf) (PDF). Archived from the original (http://www.aph.gov.au/hansard/joint/commttee/j2408.pdf) (PDF) on 8 June 2011. Retrieved 19 August 2016., Official Committee Hansard, Joint Standing Committee on Treaties, 9 August 1999. Commonwealth of Australia.
69. Schmid, Gerhard (2001-07-11). "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))" (https://fas.org/irp/program/process/rapport_echelon_en.pdf) (PDF). Retrieved 2018-08-06.
70. Staunton, Denis (1999-04-16). "Electronic spies torture German firms" (https://www.irishtimes.com/business/electronic-spies-torture-german-firms-1.174447). *The Irish Times*. Retrieved 2018-08-06.
71. Gunn, Angela. "Security goes to the movies: The Bourne Ultimatum" (http://www.computerworld.com/s/article/9029059/Security_goes_to_the_movies_i_The_Bourne_Ultimatum_i_). *Computerworld*. Retrieved 30 April 2014.

External links

- Campbell, Duncan (Aug 3, 2015). "GCHQ and Me, My Life Unmasking British Eavesdroppers" (https://theintercept.com/2015/08/03/life-unmasking-british-eavesdroppers/). *The Intercept*.
- "Paper 1: Echelon and its role in COMINT" (http://www.heise.de/tp/artikel/7/7747/1.html). *Heise*. May 27, 2001.
