Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Echelon: The Danger of Communication in the 21ST Century

Hidden from public scrutiny, a monolithic array of technology awaits your next conversation. It is a global network of computers used to automatically intercept and sort through millions of messages. In essence, it is the true life form of what George Orwell referred to as Big Brother in his classic 1984. For years now, Echelon has been the target of many a debate. Articles, speeches, white papers and even a few books have been written on the subject and its wide spread among the "Conspiracy Theory" Community. However,...

Copyright SANS Institute

Author Retains Full Rights

AD

# ECHELON

## THE DANGERS OF COMMUNICATION IN THE 21ST CENTURY

An original submission by Chad Yancey
for
SANS Security Essentials GSEC training version 1.3

Friday, February 1, 2002

© SANS Institute 2002, Author retains full

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## TABLE of CONTENTS

**Forward**…….……. 3

**A Brief History**……... 4

**The Network**
What it is, what it is not……... 5
Locations……..… 5
Equipment…… 7
How it works…… 8

**The Problem**……... 10

**Domestic Spying**
Encryption and the NSAKEY……. 11
Carnivore..……..…….. 12
Magic Lantern……...…… 12

**Commercial Spying**……... 13

**Conclusion**…….. 14

© SANS Institute 2002, Author retains full rights.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Forward

Hidden from public scrutiny, a monolithic array of technology awaits your next conversation. It is a global network of computers used to automatically intercept and sort through millions of messages. In essence, it is the true life form of what George Orwell referred to as *Big Brother* in his classic *1984*.

For years now, Echelon has been the target of many a debate. Articles, speeches, white papers and even a few books have been written on the subject and its wide spread among the "Conspiracy Theory" Community. However, what you read may not necessarily always be the truth. Through my research, I have found many denials and allegations reaching back as far as three decades. One thing is fact, Echelon does exist, but to what extent may never be known.

In this paper, I will show you how governments are using this technology to gain and collect information on not only political or military interests, but that they are suspected of using this system on common citizens. I will provide historical background information, the locations of suspected intercept stations and details of suspected activity. In the end, I hope that you will better understand the workings of Echelon and the potential danger that it poses to communication in the 21st Century.

© SANS Institute 2002, Author retains full rights.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## A Brief History

In years past, information was normally considered secure if an individual whispered it to another, or wrote something down on paper. In today's reality, a whisper can be monitored, and your e-mail, even though encrypted, can be intercepted and read. In order to fully explain what ECHELON is and how it came about, we will need to start our journey by going back at least six decades.

During World War II, the use of encryption, the science of making something secret, played a vital role in insuring the integrity of information. Germany's use of the Enigma gave them the ability to converse with utmost impunity. And the use of the Navajo language, long thought to have been forgotten, did the same for U.S. Marines in the Pacific Theater. Although these two examples of using cipher have some things in common, more importantly, there is one thing they do not. The Enigma was eventually compromised and the Wind Talkers were not.

The end of World War II brought new meaning to national security for many countries around the world. The war had tightened the alliance between several nations, and yet expanded fears with others. With the onset of the Cold War, it was necessary for countries to form ties with one another to insure the survival of their nations.

Communication via radio waves made it possible to send information transcontinental. However, the medium was not secure and anyone else could listen in as well. Thus, the use of radio transceivers gave new importance to the development of encryption.[1]

In 1948, a secret agreement (UKUSA) between the United States and the Government Communications Head Quarters (GCHQ) of England was formed to intercept communications. This agreement's foundation was in the earlier Britain USA Communications Intelligence (BRUSA COMINT) agreements of May 17, 1943. From 1984 forward, the Communications Security Establishment (CSE) of Canada codenamed CLASSIC BULLSEYE, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand[2] joined the U.S. and the U.K. in operating communications satellite (COMSAT) interception. Other countries later became third party participants by developing Signals Intelligence (SIGINT) and aligning themselves with the already successful UKUSA agreement. The details of this agreement are still classified today.

The National Security Agency (NSA) was not formed until 1952 by presidential directive under U.S. President Harry Truman. The original directive gave the NSA authorization for SIGINT and Communications Security (COMSEC). U.S. President Ronald Reagan further added directives to the NSA in 1984 by adding information systems security, and again in 1988 with the addition of supporting combat operations for the Department of Defense.[3]

Today, the NSA is undoubtedly the leader of both the UKUSA agreement and Echelon. They are the largest global employer of mathematicians, and have some, if not all, the best code breakers available. In its primary role, the NSA is responsible for developing the encryption to


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

protect the national security of the United States. However, in its later role, the NSA became responsible for the exact opposite. As the leading agency for Echelon, the NSA is responsible for creating surveillance and code breaking technology, directing cooperating agencies to their targets, and providing tools and training to those cooperating agencies to intercept, process, and analyze SIGINT.[4]

## The Network - What it is, what it is not

Most sources will elaborate on how Echelon is a complex system of intercept stations positioned strategically across the world to capture every satellite, microwave, fax, e-mail, cell phone call, etc. Duncan Campbell attempts to dispel this notion in his article "Inside Echelon"[5], by denying that Echelon has the capability to do this. "Nor is equipment available with the capacity to process and recognize the content of every speech message or telephone call."[6] However, "the American and British-run network can, with sister stations, access and process most of the world's satellite communications, automatically analyzing and relaying it to customers who may be continents away."[7]

The largest and most complex SIGINT is run by the NSA, though other nations have recently constructed their own. Among them, Russia, China, France, Denmark, Germany, Japan, Norway, South Korea, Turkey, the Netherlands and Switzerland have developed SIGINT capabilities "to obtain and process intelligence by eavesdropping on civil satellite communications."[8]

## The Network - Locations

Most of Echelon is directed to intercept data from Intelsat and Inmarsat (the maritime satellite system), which are responsible for most of the worlds phone and fax communications. The twenty or so Intelsat satellites are on a geo-stationary orbit locked onto a particular azimuth at the equator.[9] Although these satellites do primarily carry civilian traffic, they also distribute government communications to Echelon.

Morwenstow, England was the first facility constructed for the specific purpose of interception. Yakima, Washington soon followed. Both sites were responsible for interception of data from Intelsat satellites. However, with the introduction of the new 701 and 703 series satellites, data acquisition was prohibited from Southern Hemisphere signals. Because of this, additional interception sites were constructed in Australia and New Zealand.[10]


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Today, the Yakima site intercepts communications from the Pacific Ocean within the Northern Hemisphere and the Far East. The Morwenstow site targets the Atlantic and Indian Oceans. Sugar Grove in West Virgina, targets North and South America. The Waihopai, New Zealand and (*Figure 1*) and Geraldton, Australia sites cover Asia, the South Pacific and the Pacific Ocean in the Southern Hemisphere.[11] It is rumored that construction is near complete for a site in Ireland, pending that country's forthcoming membership into UKUSA.[12]

**Figure 1** **Source:** ***ZDNet***

**Figure 2** **Source:** ***Duncan Campbell***

Satellites that carry Russian and regional communications are monitored from sites in Menwith Hill, England (*Figure 2*), Shoal Bay, Australia, Leitrim, Canada, Bad Aibling, Germany, and Misawa, Japan.[13] It is speculated that Shoal Bay intercepts Indonesian satellites and that Leitrim intercepts communications from Latin America, including the Mexican telephone company Morelos.[14]

In 1998 and 1999, proof of the existence of Echelon was obtained by Dr. Jeff Richelson, a U.S. intelligence specialist of the National Security Archive, in Washington D.C. Dr. Richelson used the Freedom of Information act to obtain documents from the U.S. Navy and U.S. Air Force that confirmed the existence of five sites. The first site confirmed, Sugar Grove in West Virginia, was established in 1990 as an "Echelon training department". A 1990 satellite photograph of Sugar Grove showed four antennas located at the site. However, by 1998 this had grown to nine antennas. The documents further confirmed the existence of Yakima, Washington; Sabana Seca in Puerto Rico, Guam, and Misawa, Japan.[15]

During the Vietnam conflict, Britain was to remain neutral, however British operators at the GCHQ intercept station no. UKC201 at Little Sai Wan, Hong Kong intercepted and reported North Vietnamese air defenses to the United States.[16]

Located in North Yorkshire, England, lies the largest spy station in the world. Menwith Hill has under current deployment twenty-five satellite receiving stations, 1,400 United States NSA personnel and 350 U.K. Ministry of Defense staff. In 1966, the NSA obtained the lease for the



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

base and has continued to expand the base ever since. It has most recently become the topic of discussion by the European Parliament who are convinced that the station is being used for civilian surveillance and economic espionage by the United States.

Perhaps their fears were not in error. James Woolsey, who headed the CIA from 1993-95, has admitted that the U.S. secretly collects information on European firms. In the Wall Street Journal he wrote: "That's right, my continental friends, we have spied on you because you bribe."

**Figure 3**

## The Network – Equipment

Several ground based sites are scattered around the globe, most of which are located on military bases or spy bases. However, a major portion of the Echelon system and U.S. spy network is comprised of satellites. Satellites have been launched by the NSA in cooperation with other members of UKUSA, the National Reconnaissance Office (NRO) and the Central Intelligence Agency (CIA). Although some of the ground based downlink reception stations are based on foreign soil, they are ultimately controlled by the United States. The two primary downlink sites are located at Menwith Hill, England and Pine Gap, Australia.[17] The following is an example of satellites in current use by Echelon.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

| SATELLITE | NO. | ORBIT | MANUFACTURER | PURPOSE |
|---|---|---|---|---|
| Advanced KH-11 | 3 | 200 miles | Lockheed Martin | 5-inch resolution spy photographs |
| LaCrosse Radar Imaging | 2 | 200-400 miles | Lockheed Martin | 3 to 10 foot resolution spy photographs |
| Orion/Vortex | 3 | 22,300 miles | TRW | Telecom surveillance |
| Trumpet | 2 | 200-22,300 miles | Boeing | Surveillance of cellular phones |
| Parsae | 3 | 600 miles | TRW | Ocean surveillance |
| Satellite Data Systems | 2 | 200-22,300 miles | Hughes | Data Relay |
| Defense Support Program | 4+ | 22,300 miles | TRW/Aerojet | Missile early warning |
| Defense Meteorological Support Program | 2 | 500 miles | Lockheed Martin | Meteorology, nuclear blast detection |

**Table 1 Source: MSNBC** [18]

Ground based interception takes place as well. However, these are primarily located in areas where embassies or large concentrations of microwave medium are found. Applied Signal Technology manufactures the Model 128B TDC Channel Analyzer, a cell phone monitor capable of processing 12,000 channels at once.[19]

Rupert Goodwins, a reporter for ZDNet UK, in his June 29, 2000 article "Echelon: How it works", speculates that the system uses commercial off-the-shelf (COTS) equipment and that it is known to use IP and very strong encryption with dedicated fiber and satellite channels signals between sites.

## How it works

Espionage is a dark art. To ascertain who is doing what to whom may be near impossible. The cloak of the Echelon system is so complex, the truth may never be known even by the parties involved. Given this, it is still probable to construct a reasonable blueprint of the inner workings of this system. However, what is fact and what is fiction all depends on who you ask. More than likely, the truth lies somewhere in between.

The operation is very compartmentalized. An individual working in one facility has no idea of what the directive is for another office on the same floor, much less an adjacent facility.

The function of Echelon is to intercept, analyze and distribute information. Most of this information is simply absorbed from the sky, while other information is collected by physical taps. The collected information is analyzed for key content through Echelon dictionaries, such as


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Menwith Hill's SILKWORTH. These dictionaries include key words, phone and fax numbers voice prints and optical character recognition (OCR). MAGISTRAND, PATHFINDER and VOICECAST are all state-of-the-art programs written specifically for sifting through the enormous amounts of information.[20] Data that matches an entry in one of the dictionaries is recorded for further analysis. It is important to note here that not all data is recorded. Most data is filtered, and that is the strong point of this system.

Each station maintains it's own dictionaries, and each dictionary is maintained by a Dictionary Manager. Only the Dictionary Manager has the ability to add/delete/modify the search criteria.[21]

Data that has been analyzed and found to be of importance is forwarded to the respective government agency: ALPHA-ALPHA (GCHQ), ECHO-ECHO (DSD, INDIA-INDIA) (GCSB), UNIFORM-UNIFORM (CSE), and OSCAR-OSCAR (NSA).[22]

Analysts from the respective agencies review the data from the previous day. As the data is analyzed and decrypted, it is compiled into three different categories: reports, complete translations of recorded messages; "gists", a compilation of data meeting the same search critera; and finally summaries, compilations of both repots and gists.[23] Once the data has been categorized, it is given a classification: MORAY (secret), SPOKE (very secret), UMBRA (top secret), GAMMA (intercepts from Russia) and DRUID (intercepts sent to non-UKUSA parties).[24]

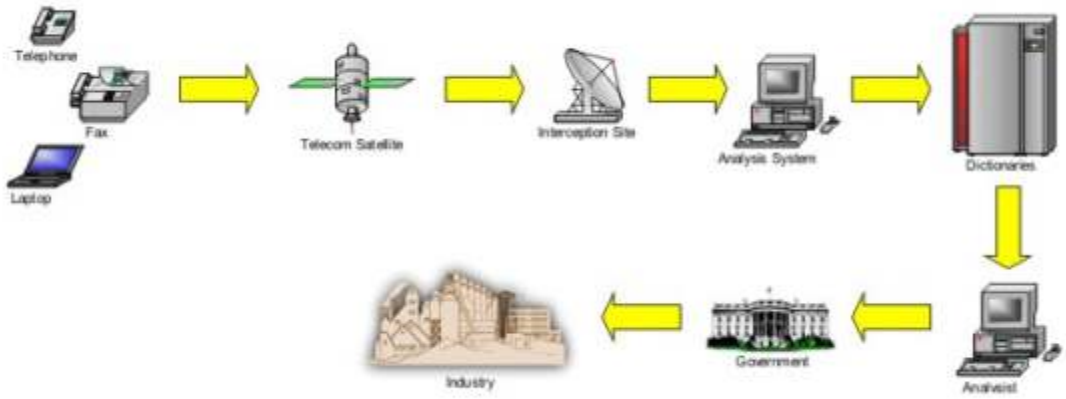


**Figure 4**

The NSA provides the center for Echelon, known as Platform. Here, other parts of the system such as Embroidery, Tideway and Oceanfront converge to exchange information. A video conference system called Gigster and a news network called Newsdealer reside on this network as well. Intelink, which is run from within Fort Meade, connects 13 different U.S. intelligence agencies along with some allied intelligence agencies to provide instant access to information. Analysts can view an atlas on Intelink's home page and simply click on the any country they desire to access intelligence information. [25]


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Along with the integration of several nations SIGINT networks, participating members of Echelon have stationed liaison staff on each other's soil. The U.S. currently operates the Special U.S. Liaison Office (SUSLO) in London and Cheltenham. While their counterparts from GCHQ operate from within the NSA at Fort Meade.

The diplomatic communications of our friends and neighbors have been and are actively cracked today. Private companies and telecommunications targets are known as "ILC" or International Leased Carrier. After having defected to the Soviet Union, two former NSA analysts, Bernon Mitchell and William Martin, gave some insight as to what the NSA was doing:

> We know from working at NSA [that] the United States reads the secret communications of more than forty nations, including its own allies…NSA keeps in operation more than 2000 manual interception positions…Both enciphered and plain text communications are monitored from almost every nation in the world, including the nations on whose soil the intercept bases are located.
> *New York Times, 7 September 1960.*

The details from Martin and Mitchell revealed that at that time the NSA was divided into two separate groups. The first covered the Soviet Union and other communist countries. The second was called ALLO or "all other [counties]". ALLO was later renamed ROW or "Rest of the World".

Peg Newsham of Sunnyvale, California, worked for Lockheed Space and Missiles Corporation on a project internally identified as P-415. She worked on plans to expand the Echelon network, but became concerned about corruption and abuse within the organization. She reported her concerns to the U.S. Congress House Permanent Select Committee on Intelligence in 1988 and testified how she was witness to a telephone interception of U.S. Senator Strom Thurmond while employed at Menwith Hill.[26]

In 1993, a policy under President Clinton known as "leveling the playing field", the government told the NSA and CIA to act in support of U.S. businesses in seeking contracts abroad. In following the direction of the U.S., the U.K. in 1994 enabled legislation that openly identifies the directive to "promote the economic well-being"[27] of the United Kingdom.

## The Problem

Echelon, without debate, is a product of the Cold War. Unscrupulous cycles of paranoia between the U.S. and the U.S.S.R. fed the budgets for intelligence agencies on both sides. But with the erosion of the Soviet Empire, these agencies were left grasping for a new mission in order to justify their very existence.

The new mission: Terrorism. This new directive paved the way and insured that their swollen budgets would continue to flow for years to come. Terrorism provided all necessary justification to develop new systems with which to spy. The results of this effort provided the capability for


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

satellites to view the most minute detail on the ground from miles above and submarines that are able to tap into undersea communications cables.[28]

Today, there is a concentrated effort by agencies to defend Echelon. Yet, events such as the Oklahoma City bombing and most recently the 9/11 attack, give undeniable testimony for the necessity to monitor any force that would use such random acts of violence as political weapons to bring harm to the U.S.

As citizens of the U.S., we must still abide by our Constitution despite the existence of such threats. The surveillance of U.S. citizens for reasons of political affiliation or economic gain is in direct violation of the First, Fourth and Fifth Amendments. Yet our Constitution is regularly obstructed by countless arguments given by skillful lawyers employed by these agencies. This happens because our trusted officials pay little or no attention to the abuses.

## Domestic Spying – *Encryption and the NSAKey*

As we enter the 21st century, world communication gets easier by the day. But are we compromising privacy for ease of use? The NSA probably does not agree. They spend countless man-hours leaning on manufacturers of software, switches and routers that include encryption in their products. Ever wonder why we have to contact the Department of Commerce, Bureau of Export Administration (BXA) to ask for permission to send an off-the-shelf encryption product overseas? It's simple. The NSA wants to ensure that the government has access to your data. Until recently, the official acceptable encryption allowed for exportation was 40-bit. The standard has been raised slightly, but not by far. Today, companies can provide mass market encryption commodities and software with key lengths not exceeding 64-bits for the symmetric algorithm.[29]

To overcome this shortcoming in encryption, the Clinton administration allowed the export of products with strong encryption by any manufacturer that would provide a "key-recovery" to the government. This however allows the government access to encrypted data with the knowledge of the end-user.

For those interested, take a look at the BXA website for more information located at http://www.bxa.doc.gov/encryption/. To obtain permission to export is cryptic at best. Do not make a mistake in your submission. It could mean that you will have to start the entire process over. And when the average wait time is six months, your product may be obsolete before you are authorized to ship it.

CNN reported in 1998, that the industry was facing a year-end deadline by the NSA to add a government approved back door into their products or face losing their export privileges. Because almost every network switch, router and operating system today includes some form of strong encryption, almost all major manufacturers must now answer to the NSA if it wishes to continue to export their products.[30] Ira Rubenstein from Microsoft Corp. admits that he acts as a "filter" between Microsoft and the NSA. "Any time that you're developing a new product, you will be working closely with the NSA."


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Another CNN press release from September 3, 1999 reveals that Microsoft operating systems include a back door that allows the National Security Agency to enter systems without permission of the owner. Andrew Fernandes, a cryptography expert that works for Cryptonym, says, "It turns out that there are really two keys used by Windows; the first belongs to Microsoft, and it allows them to securely load (the cryptography services), the second belongs to the NSA. That means that the NSA can also securely load (the services) on your machine, and without your authorization."[31]

Alison Giacomelli, Director of Export Compliance for VPNet Technologies, Inc., a manufacturer of IP based gateways in San Jose, CA., said, "the Bureau of Export Control is actually just a front for the NSA," insinuating that the NSA has the ultimate sign-off authority for Key Management Infrastructure (KMI) licenses.[32]

## Domestic Spying – *Carnivore*

So just how deep does the long arm of Echelon run? What agencies does it influence, or even control? In July 2000, a Congressional Statement from the Federal Bureau of Investigation (FBI), discussed the "Internet and Data Interception Capabilities Developed by the FBI".[33] This statement explains at a high level what the Carnivore system is and how it is deployed. More importantly, it names the current law under which the FBI justifies the use of Carnivore. Under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the law recognized the need for wiretaps. However, the act intended to provide a means of interception without violating a citizen's rights. Furthermore, the only crimes in which a wiretap should be utilized are bribery, kidnapping, robbery, murder, counterfeiting, fraud, narcotics or conspiracy.

Understanding that our society operates from laws much older than 1968, we must still place this in perspective. The predecessor to the Internet, the ARPANET, was but a vision in 1968. In fact, the program plan for the ARPANET, titled "Resource Sharing Computer Networks", was submitted June 3, 1968.

## Domestic Spying – *Magic Lantern*

MSNBC reported in November of 2001, that the FBI is developing yet a new program codenamed "Magic Lantern". This software is capable of inserting a virus onto a machine and obtaining encryption keys enabling the FBI to read data that has been encrypted on a suspect's hard drive. The development of this software was brought about due to the widespread use of encryption.[34] As details of the Carnivore systems became apparent, the use of private key encryption became more prevalent. The use of such technology raised an interesting question: Have our civil rights been violated?

In an interview by MSNBC, Rep. Dick Armey (R-Texas) said that Magic Lantern did not raise the Fourth Amendment issue regarding "Search and Seizure" as Carnivore had, because Magic Lantern would target an individual whereas Carnivore targets the customer base of a particular Internet Service Provider (ISP).[35]


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The deployment and oversight of this technology should be taken with skepticism. The technology is here and available for deployment. However, are the agents responsible for the oversight and use of this technology properly trained? It has long been known that agents are typically playing catch up with the hacking community, and do not always realize their mistake until it is too late.

The attorney for the Electronic Privacy Information Center and longtime critic of Carnivore, David Sobel said in an interview with MSNBC: "It is a matter of what protections are in place. At this point, the best documented case is Scarfo, and that raises concern". During the investigation of Nicodemo Scarfo, the FBI broke into Scarfo's apartment and installed software enabling them to steal the encryption keys from the suspect's PC. Sobel added "the federal magistrate who approved the technology in Scarfo had no understanding of what this thing was. I hope there can be meaningful oversight (for Magic Lantern)".[36]

At present, or at least before the introduction of the USA Patriot Act, Echelon fell under the Foreign Intelligence Surveillance Act (FISA) of 1978, which allowed for the investigation of U.S. citizens. Under FISA, if there is information indicating that a U.S. citizen is a spy, a terrorist, a saboteur or an accomplice, a judge may determine that citizen a foreign agent.[37]

On the horizon, a new wireless technology called ultra-wideband or pulse wireless, promises to make many transmissions virtually undetectable.[38] Historically speaking however, this technology along with its progeny will most likely follow the measure, counter measure model and soon be broken as well.

## Commercial Spying

Within the Department of Commerce, the Office of Intelligence Liason receives intelligence reports regarding pending international trade agreements that it discretely forwards to U.S. companies that may benefit from the information. In January of 1993, U.S. President Clinton added to this scrupulous activity by creating the National Economic Council, which forwards intelligence reports to "select" companies. These "select" companies - Lockheed, Boeing, Raytheon, Loral and TRW - are often the same companies that are actively involved in the creation, manufacture and operation of the Echelon systems.[39]

In 1993, U.S. President Clinton requested the CIA to conduct surveillance on Japanese automobile manufacturers who were designing zero-emission cars. This information was forward to "The Big Three" (GM, Ford and Chrysler).[40]

In 1994, Duncan Campbell, a British investigative journalist, charged that the U.S. utilized Echelon to beat the European consortium Airbus in a major plane deal with Saudi Arabia.[41]

In 1994, Intelligence reports were forwarded to Raytheon regarding a radar system that Brazil was looking to purchase.[42]


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

But the U.S. is not the only nation that engages is such activity. In 1981, an intercepted cell phone call by the CSE regarding a grain agreement that the U.S. was going to pursue with China, gave Canada the negotiating strategy and the ability to underbid the U.S. The contract earned the Canadian Wheat Board $2.5 billion. Later that same year, the CSE intercepted another message leading to a $50 million wheat sale to Mexico.[43]

## Conclusion

With the introduction of the USA Patriot Act, passed in October 2001, deployment of this type of technology will be much easier. And although we live in an age where knowledge is power, and power can be abused, it is a necessary reality if we are to maintain our way of life. But because these operations are so secret, and are able to maintain that secrecy for decades, the governments which operate them can delude accusations with plausible denial. Nicky Hager, author of *Secret Power*, addressed the European Parliament Echelon Committee in April of 2001, and stressed a single issue: setting precedence of law over this kind of technology and the systems to follow.[44] In other words, who will watch the watchers? Freedom has always come with a price, and today that price is your privacy. But if the invasion of your privacy saves lives, keeps terrorists at bay or even thwarts a war, is it worth it? This question is one that we must each decide as we consider the Dangers of Communication in the 21st Century.

© SANS Institute 2002, Author retains full rights.



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## References


[1] Duncan Campbell, "Inside Echelon", 25 July 2000
URL: http://www.heise.de/tp/english/inhalt/te/6929/1.html (16 January 2002)
[2] Patrick S. Poole, "ECHELON: America's Secret Global Surveillance Network", 1999/2000
URL: http://fly.hiwaay.net/~pspoole/echelon.html (16 January 2002)
[3] National Security Agency, "About the NSA"
URL: http://www.nsa.gov/about_nsa/index.html (17 January 2002)
[4] See Reference Number 2
[5] See Reference Number 1
[6] See Reference Number 1
[7] See Reference Number 1
[8] See Reference Number 1
[9] Intelsat, "Satellites, Coverage Maps", 2001
URL: http://www.intelsat.com/satellites_coveragemaps.asp (21 January 2002)
[10] Hager, Nicky, Secret Power: New Zealand's Role in the International Spy Network, New Zealand: Craig Potton Publishing, 1996. p. 28.
[11] See Reference Number 2
Ibid., p.35.
[12] Rupert Goodwins, "Echelon: How it works", ZDNet UK, 29 June 2000
URL: http://news.zdnet.co.uk/story/0,,s2079849,00.html (16 January 2002)
[13] See Reference Number 2
Ibid.
[14] Marco Campagna, Un Systeme De Surveillance Mondial, Cahiers de Television (CTV-France), June 1998; Peter Hum, I spy, the Ottawa Citizen, 10 May 1997.
[15] Richard Barry and Duncan Campbell, "Echelon: Proof of its existence", 29 July 2000
URL: http://news.zdnet.co.uk/story/0,,s2079847,00.html (16 January 2002)
[16] See Reference Number 1
[17] See Reference Number 2
[18] Robert Windrem, Spy Satellites Enter Net Dimension, MSNBC and NBC News, 8 August 1998
URL: http://www.msnbc.com/news/185953.asp
[19] See Reference Number 12
[20] See Reference Number 2
[21] Hager, Nicky, Secret Power New Zealand's Role in the International Spy Network, New Zealand: Craig Potton Publishing, 1996. p. 49.
[22] Bamford, James, The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization, New York: Penguin Books, 1983, pp. 138-139
[23] Hager, Nicky, Secret Power New Zealand's Role in the International Spy Network, New Zealand: Craig Potton Publishing, 1996. p. 45.
[24] See Reference Number 2
[25] Martin, Frederick, Top Secret Intranet: How U.S. Intelligence Built Intelink – the world's largest, most secure network, Prentice Hall, 1999
[26] See Reference Number 1
[27] GHCQ: British Intelligence
URL: http://www.gchq.gov.uk/index.html (23 January 2002)
[28] Ball, Desmond and Richelson, Jeffrey, The Ties that Bind: Intelligence Cooperation Between the UKUSA Countries, Boston: Allen & Unwin, 1985, pp. 223-224
[29] Department of Commerce, Bureau of Export Administration, "FAQ", 19 October 2000
URL: http://www.bxa.doc.gov/encryption/Oct2KQandAs.html (18 January 2002)




© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[30] Ellen Messmer, "The long, strong arm of the NSA", 27 July 1998
URL: http://packetstorm.decepticons.org/crypt/nsa/arm-of-nsa.txt (17 January 2002)
[31] CNN.com, "Crypto expert: Microsoft products leave door open to NSA", 3 Sepember 1999
URL: http://cnn.com/TECH/computing/9909/03/windows.nsa/ (17 January 2002)
[32] See Reference Number 30
[33] Congressional Statement, Federal Bureau of Investigation "Internet and Data Interception Capabilities Developed by FBI", 24 July 2000
URL: http://www.fbi.gov/congress/congress00/kerr072400.htm (16 January 2002)
[34] Bob Sullivan, MSNBC, "FBI software cracks encryption wall", 20 November, 2001
URL: http://www.msnbc.com/news/660096.asp
[35] See Reference Number 34
[36] See Reference Number 34
[37] Robert Lemos, ZDNet US, "Echelon fears could force new laws for America", 29 June 2000
URL: http://news.zdnet.co.uk/story/0,,s2079848,00.html (16 January 2002)
[38] See Reference Number 12
[39] See Reference Number 2
[40] Dreyfuss, Robert, Company Spies, Mother Jones, May/June 1994
[41] Ian Black, "Britain accused of aiding industrial espionage by US," The Guardian, 31 March 2000
URL: http://www.guardian.co.uk/international/story/0,3604,178445,00.html (18 January 2002)
[42] Bowman, Tom and Shane, Scott, Battling High-Tech Warriors, Baltimore Sun, 15 December, 1995
[43] Frost, Mike and Graton, Michel, Spyworld: How C.S.E. Spies on Canadians and the World, Toronto: Seal/McClelland-Bantam, 1995, p.224-227
[44] Nicky Hager, "Nicky Hager Addresses the Echelon Committee", Scoop, 17 May 2001
URL: http://www.scoop.co.nz/mason/stories/HL0105/S00104.htm (24 January 2002)


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Melbourne 2013** | **Melbourne, AU** | **Sep 02, 2013 - Sep 07, 2013** | **Live Event** |
| **SANS Capital City 2013** | **Washington, DCUS** | **Sep 03, 2013 - Sep 08, 2013** | **Live Event** |
| **Network Security 2013** | **Las Vegas, NVUS** | **Sep 14, 2013 - Sep 23, 2013** | **Live Event** |
| **SANS Canberra 2013** | **OnlineAU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |