GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

The History, the Players and the Stakes Behind Echelon, Monitoring Technologies and Global Surveillance

by Jean-Philippe Décarie-Mathieu

GSEC Practical Assignment
Version number 1.4b – Option 1

© SANS Institute 2000 - 2005, Author retains full rights.

Summary

The collapse of the Third Reich in Europe in the mid-1940s signalled the end of a painful area for Europe and paved the way for a drastically different world in the ensuing decades. The world was left with only two superpowers – the United States of America and the Union of Soviet Socialist Republics. The inevitable clash between those two countries with drastically different ideologies unfolded in a peculiar way: a war was fought not with weapons and soldiers (mostly, at least), but with satellites and spies. This confrontation led to rapid advancements in the global surveillance field and monitoring technologies. From the UKUSA Agreement to the COMSAT stations, the possibility of John Q. Public being monitored in any time from anywhere became more than a possibility – it became reality.

The History Behind the UKUSA Agreement

The UKUSA SIGINT (United Kingdom/United States of America Signals Interception, the former name of the more well-known "Echelon") community traces its roots back during and after the events of World War II. This global conflict obviously gave a boost and created a renewal for intelligence gathering agencies and technologies from around the world. The cooperation got its start in 1940 and was later officialized on May 17 1943[1] with the still-very-secret and possibly still-active BRUS COMINT (Britain/United States Communications Interception) agreement. Information is very scarce concerning this agreement

© SANS Institute 2000 - 2005 Author retains full rights.

because, in Canada, access to documents pertaining to this alliance (and any SIGINT-related papers) requires a Top-Secret-level access.

Several years later, in 1948, an alliance was formalized between the USA, the UK and three Commonwealth nations, those being Canada, New Zealand and Australia. More nations European nations allied themselves with this entente as minor participants. Other countries, like China and Russia, also agreed to host UKUSA SIGINT stations on their soil and share communication, signals and messages that they intercepted with members of UKUSA. The People's Republic of China is hosting at least two stations that are co-operated by American Intelligence officials. Those two stations were once directed at Russia and employed more than 54,000 people to maintain the FAPSI ("Federal Agency of Governmental Relations and Information"), which is the Russian equivalent of the N.S.A. Over the years, several other Middle Eastern and Asian nations invested in SIGINT-related mechanisms, like Israel, India and Pakistan[2].

The UKUSA Agreement was known by many different code-names during its history, including Project 415, P415 and UKUSA. The modern day version of this monitoring system - now commonly known as 'Echelon' – traces its roots back to the early 1970s. Back then, the member countries of this surveillance project quickly realized that human operators could not process the amount of information received efficiently for long. The waves of communication received had to be addressed in an automated way. Therefore, the N.S.A. (National Security Agency) and the G.C.H.Q. (Government Communications Headquarters) planned the construction, in the late 1960s, of large satellite interception sites that would automate the process of capture electronic communications. Great Britain built the first of such station in Morwenstow (in Cornwall) and the United States constructed their own station in Yakima (in Washington).

In 1984, Australia, Canada and New Zealand joined the United States and the United Kingdom in operating COMSAT (Communication Satellite) interception stations[3]. The primary utility of COMSAT was to spy on specific individuals and countries that might potentially be a threat to the members of the UKUSA Agreement. Indonesia and North Korea were targeted, along with India and Pakistan (to watch the evolution of the countries' respective nuclear program).

More recently, better public awareness on the interception system Echelon has raised the ire of civil liberties advocates, politicians and activists. On October 21 1999, a large number of netizens organized sort of a mock protest to disturb the activities of Echelon. The protestors added keywords that could potentially alert the monitoring system at the end of every unencrypted message they sent (examples of keywords that were used: NSA, IRA, bombs, terrorist, WTC, etc). The idea was to overload Echelon with more noise than it could handle, potentially hindering its communication monitoring capabilities. While the actual usefulness of such action is debatable, the event nevertheless garnered

© SANS Institute 2000 - 2005 Author retains full rights.

the attention of several important news sources and, since then, October 21st is more or less recognized as Jam Echelon Day[4].

Surveillance Systems and Agencies Worldwide

The main countries participating in the UKUSA agreement are the United States of America and Great Britain. Canada, New Zealand and Australia ("second parties") later joined the pact as allied and Norway, Denmark, Germany and Turkey allied themselves with the above superpowers as "third party" participants in UKUSA.

The major SIGINT agencies in the United States and Great Britain are, respectively, the National Security Agency and the Government Communications Headquarters. Each of these countries appointed senior officials to work at the other's headquarters: the United States has SUSLOs (Special U.S. Liaison Offices) in London and Cheltenham while Great Britain has a SUCKLO (Special U.K. Liaison Office) in Fort Meade, which is known as the communication interception capital of the world (also the headquarters of the N.S.A.).

The N.S.A. is subdivided into smaller agencies, some which cooperate with other holdings of the American and British governments, like the DDOJOCC (Department of Defence Joint Operations Centre Chicksands) at Chicksands, England which was set up in 1976. The DDOJOCC main job was to intercept diplomatic and civilian messages. Two targets of this centre were the French Diplomatic Traffic and the Italian Diplomatic Signals.

China also runs its own sorts of surveillance systems. The VTMS (Vessel Traffic Management System) is targeted more at naval craft and communications. On April 9 2001, Human Events journalist Terence Jeffrey spoke about that particular monitoring system[5]:

> "*The system is capable of detecting, identifying, monitoring and communicating with ships moving through the Qiongzhou Channel.*"

It is interesting to note that Lockheed Martin, the number one private contractor of the United States Department of Defence, built this surveillance arrangement. The VTMS could technically be used by the People's Republic of China to spy on Taiwanese ships (military or civilian), even thought the United States government fully supports the Taiwanese regime.

Several other countries in the world have surveillance agencies and/or monitoring technology available. Germany, for example, has the B.N.D.

© SANS Institute 2000 - 2005 Author retains full rights.

("Bundesnachrichtendienst," which translates to "Federal Information Service"), an intelligence gathering agency that has been in service for more than half a century; Israel has three such organisations (Mossad, which handles intelligence collected outside of Israel, Shin Bet, which processes interior data and Aman, which is charged with handling military intelligence) and France's S.G.D.N. (Secretariat General de la Defense Nationale) conducts surveillance and communication-gathering tasks for the French government and for the private sector.

Echelon - Truth or Fiction?

If you were to listen to American and British government officials, they would tell you that Echelon is pure fiction; if you were to take the word of dissidents and even conspiracy theorists, you would hear that Echelon is not only a reality, but it can also intercept all e-mail, telephone and fax communications in Europe, America and virtually everywhere else in the networked world. What should we make of this? Who is telling the truth and who is lying? Is it possible that people are purposely spewing out disinformation on this subject?

On September 6, 1960, two former National Security Agency employees-turned-defectors convened a press conference in Moscow, Russia. Mathematicians William H. Martin and Bernon F. Mitchell announced to the world that the United States was spying on the communications of its allies and enemies[6]:

> "*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 intercept 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.*"

Christopher Andrew, author of "The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB," told the story of that press conference to ABC journalist David Ruppe in 1999[7]:

> "*[William] Martin and [Bernon] Mitchell, two defectors … actually give a press conference in Moscow in 1960 and mention the names of sort of 30 powers and allies [of the United States] whose codes were being broken at the moment by the United States [...]* "

To this day, the reason behind the pair's defection to the Soviet Union remains unclear. In fact, there is little information available about the two analysts, but James Winchester writes about what is known on the two former Fort Meade's

© SANS Institute 2000 - 2005 Author retains full rights.

employees[8]:

> "*[T]hey had knowledge of every American listening post around the world. Their flight behind the Iron Curtain compromised the entire network of U.S. radio intelligence.*"

Depending on whom you listen to, there was, during the Cold War, between 30 and 40 nations that were being spied on, including the United States of America. This is interesting to note, considering that the Fourth Amendment in the Bill of Rights criminalizes any intrusion of privacy (in this case, electronic surveillance) on the American people by their own government[9].

Former N.S.A. Director Lieutenant-General Lew Allen also had the following to say on August 8 1975 regarding domestic and foreign communication interception[10]:

> "*The N.S.A. systematically intercepts international communications, both voice and cable [...] Messages to and from American citizens have been picked up in the course of gathering foreign intelligence.*"

Those actions were part of a joint project (nicknamed "Operation Shamrock") by the United States and by Britain that lasted decades. Operation Shamrock got its start during a post-Great-War era (in 1920) in the United Kingdom and during the last days of World War II (in 1945) for America. The American Congress finally exposed operation Shamrock during the investigations related to the Watergate scandal that led to the re-election and, ultimately, the resignation of Richard Nixon.

While the statements made by Martin, Mitchell and Allen embarrassed the intelligence gathering agencies of the United States by accusing them of intercepting/cracking foreign and, especially, home-soil communications (something the American government has always denied it was doing), it still did not prove that a global surveillance system was brewing. It did not confirm either that an alliance between certain nations of the Commonwealth and the U.S.A. was taking place.

Enter Bruce McIndoe. This intelligence analyst was employed by the National Security Agency for more than 10 years - from 1987 to 1998 - where he worked on Echelon and, later, on Echelon II, an upgrade of sorts to the original monitoring system. He is now the second in command and co-founder of "IJet Travel Intelligence," a private American espionage agency that works with former employees and spies from difference active and expired agencies (N.S.A., K.G.B., for example). On May 2002, McIndoe had this to say about Echelon and the United States Department of Defence to Bo Elkjaer and Kenan Seeberg, reporters for the Danish paper "Ekstra Bladet"[11]:

© SANS Institute 2000 - 2005 Author retains full rights.

"*No system of such enormous magnitude would only be used for a single purpose. They [the Department of Defence] use it for everything they can, if they feel it's necessary. Whenever they need to exploit its potential, they do it.*"

McIndoe also revealed interesting facts concerning the technology used by the N.S.A. that would confirm Echelon's voice/text recognition capabilities[12]:

"*A lot of the technology developed at the NSA will sooner or later find its way into civilian life. Things like word spotting, automatic translation, language recognition and so on.*"

Geopolitical Aspect of Echelon

Britain's official zone of control concerning Echelon's signals interception covers Africa and Europe up to the Ural Mountains. Canada covers the northern latitudes and the Polar Regions, while Australia and New Zealand are monitoring Oceania.

The following is a large (but by no means complete) list of the countries participating in Echelon and most of the well-known UKUSA SIGINT stations under their control. It lists the administrative body in charge of certain stations and in what country (or countries) these are being administered.

Note: The information in this section has been taken and assembled from Duncan Campbell's report on Echelon that was published in 2000[13]. Relevant information has been added as a complement to the facts below.

Stations Administered by the United States located in:

Central and southern Germany;
Turkey;
Italy;
Spain;
Yakima, WA;
Sugar Grove, WV;

Note: Yakima was the site of the second Echelon surveillance station.
Note: Timberline II, an upgraded SIGINT system, was installed at Sugar Grove in 1990.

© SANS Institute 2000 - 2005 Author retains full rights.

Stations Administered by the USAF (United States Air Force) located in:

Chicksands, England;
San Vito dei Normanni, Italy;
Karamursel, Turkey;
Bases in the Philippines;
Misawa, Japan;

Note: The US Air Force installed, in 1964, at the locations above, 500-meter wide arrays that were code-named "Iron Horse," or FLR-9 stations. According to the Federation of American Scientists, the FLR-9 arrays use the ionosphere (the part of the upper atmosphere where there is sufficient electron density to influence to propagation of radio and electromagnetic signals) to “bounce” high-frequency radio transmissions to receivers over the horizon, thus significantly aiding in the exchange of information[14].

Stations Administered by the US Navy located in:

Rota, Spain;
Bremerhaven, Germany;
Edzell, Scotland;
Guam;
Puerto Rico;

Note: The array located at Puerto Rico is specifically targeted at Cuba.
Note: The locations above contain similar arrays that are installed at stations administered by the USAF.

Stations Administered by the United Kingdom located in:

Germany;
Austria;
Iran;
Kagnew Station at Asmara (Eritrea);
Little Sai Wai, Hong Kong, China;
Cupar, Scotland;
Morwenstow, Cornwall;
Menwith Hill, central England;

Note: the station in Eritrea was closed in 1970 (it was a former US-operated station).

© SANS Institute 2000 - 2005 Author retains full rights.

Note: the monitoring base in Little Sai Wai is classified as interception station UKC201.
Note: Morwenstow was the site of the first Echelon monitoring station.
Note: The station in Menwith Hill is the largest surveillance station outside the United States.

Stations Administered by Australia located in:

Kojarena, Geraldton (near Perth);
Shoal Bay, Northern Territories;

Note: According to Australian sources, the interception station located at Shoal Bay is NOT part of the Echelon program. Officials say that this is because the Australian government does not want to allow the United States and Great Britain to be able to tap into the raw data collected directly.

Stations Administered by New Zealand located in:

Waihopai;

Note: In 1996, a New Zealand TV crew was able to approach the station at Waihopai close enough to make a startling discovery – the station seemed to be operating almost automatically, without the help of humans. That surveillance station covers communications over the south Pacific.

Other locations and countries administering stations:

Bermuda;
Ascension;
Cyprus;
Gibraltar;
Iraq;
Singapore;
Hong Kong;
Sabana Seca (Puerto Rico);

Conclusion

The ubiquity of the intelligence-gathering surveillance technology that is Echelon

© SANS Institute 2000 - 2005 Author retains full rights.

has reached a level of pervasiveness unequalled by any organisation or individual in the history of the world. The very existence of such a monitoring system has far-reaching implications as far as personal liberties are concerned: a potential loss of privacy on a global scale could happen, information gained by using Echelon could also be used for blackmailing, racketeering and other illegal activities and an "allied hegemony" or sort could be born out of the alliance between the primary members of the UKUSA Agreement, something that could be detrimental to other countries around the globe. However, like the very existence of Echelon, the implications raised by such a system have and will be debated. While it is true that, in theory, anyone could potentially be a target of Project 415, would the powers that be really take time to investigate John Q. Public, just for the fun of it? Could such a broad-scale surveillance help resolve international problems, like terrorism? Does the good points out weight the bad ones? Until those questions are answered, Echelon will remain an integral part of our digitized world, whether we like it or not.

Bibliography

[1] Richelson, Jeffrey T. and Ball, Desmond. The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries. Allen & Unwin, 1985. 137 - 138.

[2] European Parliament. Development of Surveillance Technology and Risk of Abuse of Economic Information, Volume 5: The Perception of Economic Risks Arising from the Potential Vulnerability of Electronic Commercial Media to Interception. Luxemburg, 1999. 12.

[3] Campbell, Duncan. "Inside Echelon." Heise Online/Telepolis. 25 July 2000. URL : http://www.heise.de/tp/english/inhalt/te/6929/1.html (21 October 2002).

[4] "Jam Echelon Day." Cipherwar.com. 21 October 2001. URL: http://www.cipherwar.com/echelon/ (21 October 2002).

[5] Jeffrey, Terence P. "Lockheed Built Naval Surveillance System for PRC." Human Events Online. 9 April 2001. URL: http://www.humaneventsonline.org/articles/04-09-01/jeffrey.html (21 October 2002).

[6] New York Times. 7 September 1960.

[7] Ruppe, David. "Russian Intelligence Still Matters." ABCNews.com. 14 September 1999. URL: http://abcnews.go.com/sections/world/DailyNews/andrewqna_990914.html (21

© SANS Institute 2000 - 2005 Author retains full rights.

October 2002).

[8] Winchester, James H. "America's Most Wanted Defectors." Family Weekly. 18 October 1964: 6 - 7.

[9] "U.S. Constitution – Bill of Rights." URL: http://www.law.cornell.edu/constitution/constitution.billofrights.html (21 October 2002).

[10] See **[3]**, above.

[11] Elkjaer, Bo and Seeberg, Kenan. "Echelon's Architect." Ekstra Bladet. 21 May 2002. http://cryptome.org/echelon2-arch.htm (21 October 2002).

[12] Ibid.

[13] See **[3]**, above.

[14] "AN/FLR-9." Federation of American Scientists. 31 August 1997. URL: http://www.fas.org/irp/program/collect/an-flr-9.htm (21 October 2002).

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: April 28th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS