Harvard Research and Publications International

Vol. 8 No. 1 ISSN: 1465-7508

JOURNAL OF PURE AND APPLIED SCIENCE

ECHELON TECHNOLOGY

ANTHONY ATIMA UMUKORO & OKOH LULU MAMELLO

Computer Science Department, Delta State Polytechnic, Otefe-Oghara.

Abstract

Echelon is a term associated with a global network of computers that automatically search through millions of intercepted messages for pre-programmed keywords or fax, telex and e-mail addresses. Echelon's function is to covertly intercept information and pass it to those who need to know. This breaks down into three stages: the collection of all possible intelligence, its analysis and contextualization, and its redistribution. The ECHELON system is fairly simple in design: position intercepts stations all over the world to capture all satellite, microwave, cellular and fiber-optic communications traffic, and then process this information through the massive computer capabilities.

KEYWORDS*:*

Computer, network, Echelon, System, Technology.

INTRODUCTION

ECHELON is a term associated with a global network of computers that automatically search through millions of intercepted messages for pre-programmed keywords or fax, telex and e-mail addresses. Every word of every message in the frequencies and channels selected at a station is automatically searched. The processors in the network are known as the ECHELON Dictionaries. ECHELON connects all these computers and allows the individual stations to function as distributed elements an integrated system.

Echelon is the technology for sniffing through the messages sent over a network or any transmission media, even it is wireless messages. Tempest is the technology for intercepting the electromagnetic waves over the air. It simply sniffs through the electromagnetic waves propagated from any devices, even it is from the monitor of a computer screen. Tempest can capture the signals through the walls of computer screens and keystrokes of key board even the computer is not connected to a network. Thus the traditional way of hacking has a little advantage in spying (Eames, 2012).

ECHELON, originally a secret government code name, is a surveillance program (signals intelligence / SIGINT collection and analysis network) operated on behalf of the five signatory nations to the UKUSA Security Agreement—Australia, Canada, New Zealand, the United Kingdom and the United States, also known as the Five Eyes.

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 was formally established in 1971. By the end of the 20th century, the system referred to as "ECHELON" had allegedly evolved beyond its military and diplomatic origins, to also become "...a global system for the interception of private and commercial communications."

LITERATURE REVIEW

Echelon is a term associated with a global network of computers that automatically search through millions of intercepted messages for pre-programmed keywords or fax, telex and e-mail addresses. Every word of every message in the frequencies and channels selected at a station is automatically searched.

According to Schmid (2001). The ECHELON surveillance system is a purported intelligence program that centres on the development and operation of a top-secret global surveillance network by five signatories of the UKUSA Agreement—Australia, Canada, New Zealand, the United Kingdom, and the United States. It was publicly disclosed in 1988 by investigative journalist Duncan Campbell and later expositions from journalists, government officials, and even the European Parliament seemingly confirmed its existence.

Echelon's function is to covertly intercept information and pass it to those who need to know. This breaks down into three stages: the collection of all possible intelligence, its analysis and contextualisation, and its redistribution. At each stage, there is little public information about what is actually even possible, let alone how much is used and where, but the basic systems must follow certain lines in order to work (Aldrich, 2010).

Echelon's main source of raw information is electronic signals. These can be carried on radio or on copper or fibre cables: with few exceptions, wireless signals can be best intercepted remotely while cables need a physical tap (Elkjær, 1999).

Wireless signals used by commercial and governmental concerns extend from very long wave transmissions through to microwaves, each waveband having its own characteristics. Most areas of interest are at VHF and higher frequencies, although shortwave has traditionally been heavily used and monitored by the military and intelligence agencies, its unreliability, low bandwidth and ease of monitoring has led to it falling out of fashion (Roberto, 2014).

A large part of Echelon is devoted to monitoring the Intelsat network of geostationary communications satellites, with ground stations in all of the UKUSA countries (and, rumour has it, work going on in Ireland pending that country's forthcoming membership of the club this month). There are also ancillary stations near to the official Intelsat groundstations, monitoring spillage of microwave uplinks and downlinks. Inmarsat, the maritime satellite system, has links to the American government and contains its own monitoring system, and other satellites with nominally civilian purposes may also have components linked to Echelon, the NSA or other agencies -- a tradition extant since the very first US Discovery series of satellites. Signals collected by satellite aren't analysed to any great extent in situ, instead they are encrypted and beamed down to the UKUSA's network of monitoring stations for dissection. Each station has responsibility for a specific geographic region (Hager, 1996).

Once the information is gathered in raw form, it is sifted using various systems. Echelon is famous for having so-called dictionary computers that can perform massive keyword searches on intercepted text, with the word lists being shared among all the agencies. A dictionary at the Waihopai station station, New Zealand, would look for GCHQ words alongside its own list, while one at the UK's Morwenstow station would reciprocate (Bamford, 2008).

Voice recognition remains a hotly-debated capability of Echelon. Systems capable of automatically triggering tape recordings on key words have existed for a while, but their reliability, scale and usability have never been established. Some automation is undoubtedly used, but it is unlikely to extend to full transcription of all calls (Nabbali, 2004).

History and Context of Echelon Technology

The ability to intercept communications depends on the medium used, be it radio, satellite, microwave, cellular or fiber-optic. During World War II and through the 1950s, high-frequency ("short-wave") radio was widely used for military and diplomatic communication and could be intercepted at great distances. The rise of geostationary communications satellites in the 1960s presented new possibilities for intercepting international communications (Keefe, 2005).

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.

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.

In 1981, the 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. 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."

Most reports on ECHELON focus on satellite interception. Testimony before the European Parliament indicated that separate but similar UK-U.S. systems are in place to monitor communication through undersea cables, microwave transmissions, and other lines. 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.

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. 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. Even in less-developed parts of the world, communications satellites are used largely for point-to-multipoint applications, such as video. 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.

Tempest and Echelon

Interception of communications is a method of spying commonly employed by intelligence services, whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications, although the analysis carried out in the report has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed.

The Need for an Interception System

Interception of messages is the major work for the intelligence agencies all over the world, to keep track of the spies and terrorists for preserving the security of the country from the leaking of sensitive documents and the terrorist attacks. By the work of the intelligence agencies the government is ensuring the security of the state. For that we have to enable our intelligence agencies with modern technologies like USA. For that we must setup an interception system. While developing this we have to consider about the privacy of common people and industrial organization.

The targets for the ECHELON system developed by the NSA are apart from directing their ears towards terrorists and rogue states; ECHELON is also being used for purposes well outside its original mission. In America the regular discovery of domestic surveillance targeted at American civilians for reasons of “unpopular” political affiliation or for no probable cause at all in violation of the First, Fourth and Fifth Amendments of the Constitution of America– are consistently impeded by very elaborate and complex legal arguments and privilege claims by the intelligence agencies and the US government. The guardians and caretakers of their liberties, their duly elected political representatives, give scarce attention to these activities, let alone the abuses that occur under their watch. The other ECHELON targets are political spying and industrial espionage.

The existence and expansion of ECHELON is a foreboding omen regarding the future of our Constitutional liberties. If a government agency can willingly violate the most basic components of the Bill of Rights without so much as Congressional oversight and approval, we have reverted from a republican form of government to tyranny.

While considering about the political spying we have to consider many legal issues. It consists of spying the other parties and the messages sent by them. Since the close of

World War II, the US intelligence agencies have developed a consistent record of trampling the rights and liberties of the American people. Even after the investigations into the domestic and political surveillance activities of the agencies that followed in the wake of the Watergate fiasco, the NSA continues to target the political activity of "unpopular" political groups and our duly elected representatives. While considering about the Industrial Espionage we have to discuss we have to redefine the notion of National Security to include economic, commercial and corporate concerns. Many of the major companies helped NSA to develop the ECHELON system to tackle the mammoth task for setting up the largest computing power throughout the world.

ECHELON is actually a vast network of electronic spy stations located around the world and maintained by five countries: the US, England, Canada, Australia, and New Zealand. These countries, bound together in a still-secret agreement called UKUSA, spy on each other's citizens by intercepting and gathering electronic signals of almost every telephone call, fax transmission and email message transmitted around the world daily. These signals are fed through the massive supercomputers of the NSA to look for certain keywords called the ECHELON "dictionaries."

Concerns on Echelon Technology

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. Examples alleged by the journalists include the gear-less wind turbine technology designed by the German firm Enercon and the speech technology developed by the Belgian firm Lernout & Hauspie.

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.

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"). 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".

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

- On behalf of the British Prime Minister Margaret Thatcher, the Canadian Security Intelligence Service of Canada spied on two British cabinet ministers in 1983.
- The U.S. National Security Agency spied on and intercepted the phone calls of Princess Diana 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". An official insisted that "the references to Diana in intercepted conversations were 'incidental'," and she was never a 'target' of the NSA eavesdropping.
- U.K. agents monitored the conversations of the 7th Secretary-General of the United Nations Kofi Annan.
- U.S. agents gathered "detailed biometric information" on the 8th Secretary-General of the United Nations, Ban Ki-Moon.
- 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.

At least one non-commercial journalist has already suggested that technologies likely connected with ECHELON might be used illegally, for unhuman treatment of politically repressed people.

The Workings of Echelon

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.

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 radar's capabilities, satellite's ground station's transmissions and ground-based microwave communications.

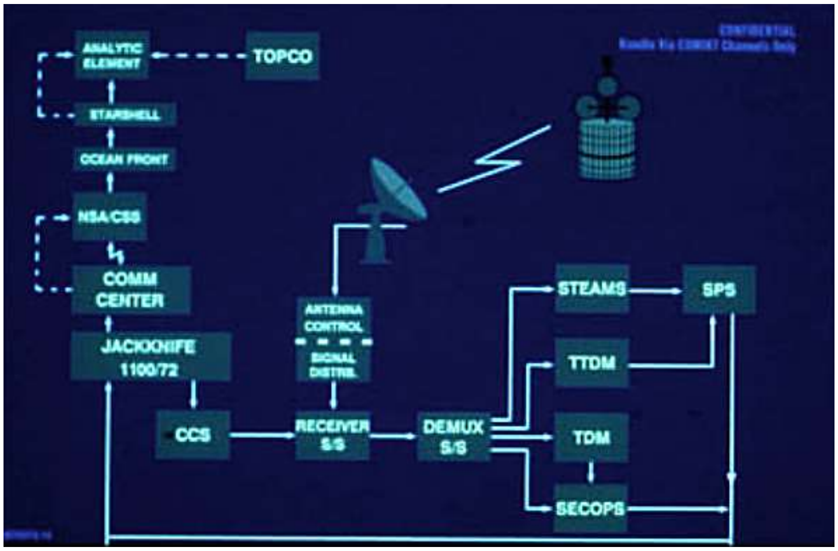

Figure 2.1, System diagram of the ECHELON satellite intercept station

DISCUSSION

Inside Echelon

ECHELON stands for NSA's (National Security Agency of America) secret Global Surveillance System developed for intercepting the messages over the world. As said in the Medias NSA is No Such Agency, but it is not the truth. This massive surveillance system apparently operates without the oversight of either Congress or the courts. Shockingly, the NSA has failed to adequately disclose to Congress and the public the legal guidelines for the project. Without those legal guidelines and an explanation of what they allow and forbid, there is no way of knowing if the NSA is using Echelon to spy on Americans in violation of federal law. In April 2000, the House Intelligence Committee held a hearing to deal with credible reports that suggest Echelon is capturing satellite, microwave, cellular and fiber-optic communications worldwide. The House Intelligence Committee intended the hearing to help ensure that ECHELON does not circumvent any requirement in federal law that the government obtains a warrant from a court before it eavesdrops on a conversation to, from, or within the United States.

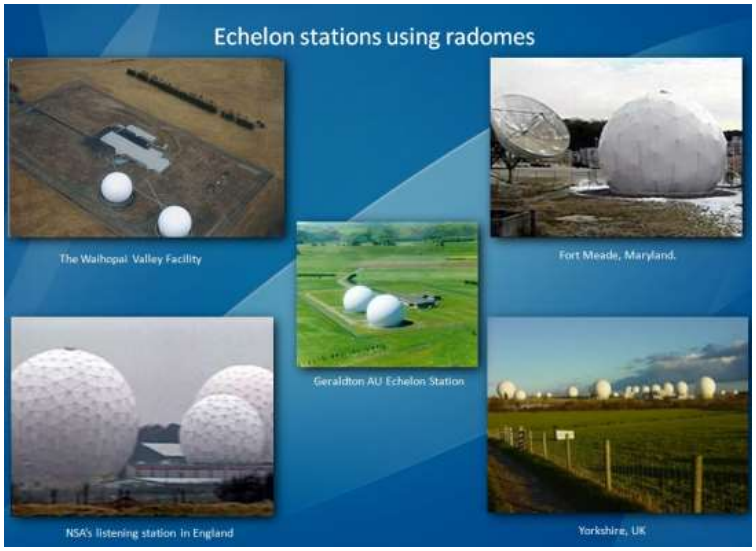
Echelon stations using radomes
The Waihopai Valley Facility
Fort Meade, Maryland.
Geraldton AU Echelon Station
NSA's listening station in England
Yorkshire, UK

Fig 3.1 Echelon stations using radomes

The ECHELON system is fairly simple in design: position intercept stations all over the world to capture all satellite, microwave, cellular and fiber-optic communications traffic, and then process this information through the massive computer capabilities of the NSA, including advanced voice recognition and optical character recognition (OCR) programs, and look for code words or phrases (known as the ECHELON “Dictionary”) that will prompt the computers to flag the message for recording and transcribing for future analysis. Intelligence analysts at each of the respective “listening stations” maintain separate keyword lists for them to analyze any conversation or document flagged by the system, which is then forwarded to the respective intelligence agency headquarters that requested the intercept.

Espionage, What Does It Means

Governments have a need for systematic collection and evaluation of information about certain situations in other states. This serves as a basis for decisions concerning the armed forces, foreign policy and so on. They therefore maintain foreign intelligence services, part of whose task is to systematically assess information available from public sources. The rapporteur has been informed that on averages this account for at least 80% of the work of the intelligence services. However, particularly significant information in the fields concerned is kept secret from governments or businesses and is therefore not publicly accessible. Anyone who nonetheless wishes to obtain it has to steal it. Espionage is simply the organized theft of information.

Uses and Applications of Echelon

In the days of the cold war, ECHELON's primary purpose was to keep an eye on the U.S.S.R. In the wake of the fall of the U.S.S.R. ECHELON justifies it's continued multi-billion dollar expense with the claim that it is being used to fight "terrorism", the catch-all phrase used to justify any and all abuses of civil rights.

With the exposure of the APEC scandal, however, ECHELON's capabilities have come under renewed scrutiny and criticism by many nations. Although not directly implicated in the bugging of the Asia Pacific Economic Conference in Seattle, the use of so many U.S. Intelligence agencies to bug the conference for the purpose of providing commercial secrets to DNC donors raised the very real possability that ECHELON's all-hearing ears were prying corporate secrets loose for the advantage of the favored few.

Given that real terrorists and drug runners would always use illegal cryptographic methods anyway, the USA led attempt to ban strong crypto to the general populace seemed geared towards keeping corporate secrets readable to ECHELON, rather than any real attempt at crime prevention.

How Echelon Surveillance System Works

The ECHELON surveillance system is a purported intelligence program that centres on the development and operation of a top-secret global surveillance network by five signatories of the UKUSA Agreement—Australia, Canada, New Zealand, the United Kingdom, and the United States. It was publicly disclosed in 1988 by investigative journalist Duncan Campbell and later expositions from journalists, government officials, and even the European Parliament seemingly confirmed its existence.

An investigation conducted by the European Parliament in 2000 provided the simplest operational description of the ECHELON surveillance system. Accordingly, intelligence organizations or agencies from the five UKUSA countries intercept transmissions using systems assembled in different parts of the world. They exchange these transmissions and continuously subject them under a keyword search.

The so-called ECHELON dictionaries contain keywords that might raise suspicion. Thus, upon intercepting transmissions, supercomputers perform a search and flag up any messages containing the suspicious keywords. The flagged transcriptions are recorded and transcribed for further analysis.

In his 1988 article published in the British magazine New Statesman, Campbell provided an overview of the earlier operational workings of the ECHELON surveillance system—which accordingly was developed after the Second World War and utilised further during the Cold War. Under the UKUSA Agreement, the signatory countries are given the task to monitor transmissions and coordinate signals intelligence in assigned regions of the world.

As mentioned, the U.S. National Security Agency supervised the entire program. It was also responsible for covering the transmissions in Soviet Union and most of the Americas. The Global Communications Headquarters of the British intelligence was responsible for monitoring and coordination in Europe, Africa, and other parts of the Soviet Union. Another listening network in Australia and the involved organizations there coordinated the monitoring of transmissions in the South Pacific and Southeast Asia.

Each participating countries operates several computer centres. As mentioned above, using supercomputers that run a particular software, the intercepted transmissions are subjected under a keyword search. These keywords include single words, phrases, and names, among others that are related to military activities, drug trafficking and other crimes, trade of embargoed goods and other dual-use technology, and economic activities.

The 2001 report based on the investigation on the European Parliament argued that long-distance technology-aided communications are possible to intercept as long as the interceptor is able to access the involved medium.

In long-distance technology-aided communication according to the report, people can use any of the following medium: air for sound waves, light for fibre optic transmission, electric current used in telegraph and telephone, and electromagnetic wave for radio communications.

Interception using the ECHELON surveillance system becomes possible through wire tapping of telecommunication lines or cables placed under the sea or the positioning of listening receiver satellites in strategic locations according to a 1996 exposition made by New Zealand journalist Nicky Hager and a 1998 report from the European Parliament, and further discussed in the 2001 report of the EP investigation.

Of course, wiretapping has become more impossible due to the developments in digital communication technology and the growing complexity of communication lines and network gateways across the globe. For example, before, the routing of global Internet communications was situated in the US. For that reason, at that time intelligence services could intercept a substantial proportion of European Internet communications. However, a small proportion of intra-European Internet communications are routed via the US.

The former director of the Defense Signals Directorate or DSD of Australia nonetheless revealed in 1999 that signatories of UKUSA use satellites positioned over Indian and Pacific oceans to intercept electronic communications. This system has become more feasible because most of the long-distance communications are sent via satellites.

Using the satellites, the system allegedly works like a giant scanner hovering satellite communications from ground stations across the globe. Upon interception, the communications are fed into supercomputers that contain the software for searching keywords and flagging suspected messages.

Further details of the result of European Parliament investigation are in the document "On the Existence of a Global System for the Interception of Private and Commercial Communications" authored by Gerhard Schmid and published in 2001. Further details of the report of Campbell are in the article "Somebody's Listening" published in 1988 in the New Statesman.

Details of the exposition of Hager are in the book "Secret Power—New Zealand's Role in the International Spy Network" published in 1996 by Craig Potton Publishing. Further details of the European Parliament report are in the article "An Appraisal of Technologies of Political Control" published in 1998. More details of the revelation of Brady are in the article "Britain and US Spy on World" authored by Duncan Campbell and Honigsbaum and published in 1999 by The Guardian.

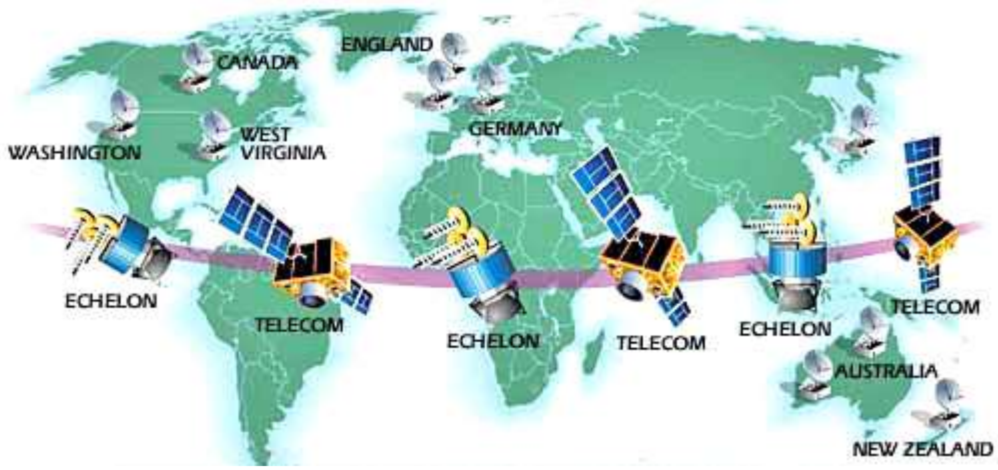

Figure 3.2, Architecture of Echelon Global Surveillance System

The Echelon Dictionaries

The extraordinary ability of ECHELON to intercept most of the communications traffic in the world is breathtaking in its scope. And yet the power of ECHELON resides in its ability to decrypt, filter, examine and codify these messages into selective categories for further analysis by intelligence agents from the various UKUSA agencies. As the electronic signals are brought into the station, they are fed through the massive computer systems, such as Menwith Hill's SILKWORTH, where voice recognition, optical character recognition (OCR) and data information engines get to work on the messages. The database containing the keywords may be huge, these huge database is called as the Dictionaries. Each station maintains a list of keywords (the "Dictionary") designated by each of the participating intelligence agencies. A Dictionary Manager from each of the respective agencies is responsible for adding, deleting or changing the keyword search criteria for their dictionaries at each of the stations. Each of these station dictionaries is given code word, such as COWBOY for the Yakima facility and FLINTLOCK for the Waihopai facility. These code words play a crucial identification role for the analysts who eventually look at the intercepted messages.

By the rise of post-modern warfare – terrorism – gave the establishment all the justification it needed to develop even greater ability to spy on our enemies, The satellites that fly thousands of miles overhead and yet can spy out the most minute details on the ground; the secret submarines that troll the ocean floors that are able to tap into undersea communications cables.

SUMMARY, CONCLUSION AND RECOMMENDATION

Summary

The interception of communication is the main function done by the intelligence agencies all over the world. The intelligence agencies are searching for the sophisticated methods for surveillance and spying from its own people and from its enemies. Here the scientists in the NSA developed the modern techniques for finding the interception of messages. And they developed a network known as the Echelon System. It made them to leap ahead of the hackers in one step.

Conclusion

Echelon is the vast network formed by NSA and its allies all over the world to intercept the messages sent through any transmission media. It plays a major role in the intelligence related work of the NSA and its allies. It uses the largest computing power of distributed systems. It uses search algorithms and sophisticated soft wares like speech recognition and OCR software. It will only preserve the states policies .This will cause the leaking of the sensitive data of the industries and it will cause harm to that companies.

Recommendation

Owing to the fact that the ECHELON technology has a major impact in network data security, I therefore recommend that the technology should used by government agencies for network security.

REFERENCES

Aldrich, R. The Uncensored Story of Britain's Most Secret Intelligence Agency, HarperCollins, July 2010. ISBN 978-0-00-727847-3, **2010.**

Bamford, J. The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America, Doubleday, ISBN 0-385-52132-4, **2008**

Eames, D. The Northwest Passage, Yakima Research Station (YRS) newsletter: Volume 2, Issue 1, January 2011 & Volume 3, Issue 7, July **2012.**

Elkjær, B. ECHELON. Ekstra Bladet. England. Ekstra Bladet `Duncan Campbell and Mark Honigsbaum (23 May 1999). "Britain and US spy on world". The Observer. (Retrieved 19 December 2013), **1999**.

Hager, N. Secret Power: New Zealand's Role in the International Spy Network; Craig Potton Publishing, Nelson, NZ; ISBN 0-908802-35-8, **1996**

Keefe, P. Dispatches from the Secret World of Global Eavesdropping; Random House Publishing, New York, NY; ISBN 1-4000-6034-6, 2005

Nabbali, T. Going for the throat. Computer Law & Security Review 20 (2): 84–97. doi:10.1016/S0267-3649(04)00018-4. It wasn't until 1971 that the UKUSA allies began ECHELON, **2004.**

Roberto K. Capitais de 4 países também abrigaram escritório da NSA e CIA". O Globo (in Portuguese), **2014**.