

THE INTERCEPTION OF COMMUNICATIONS

Jérôme Mellon

30 April 2002

Introduction

‘Signals intelligence was the best kept secret of the Cold War’, wrote Christopher Andrew. Although historians now recognize the important role it played during the Second World War, SIGINT seems to have been ignored by a lot of intelligence historians writing about the Cold War or about post-World War Two figures. We know now that signals intelligence greatly evolved in the last fifty years to become one of the principal – if not the most important – source of intelligence. The interception of communications is part of that ever-growing field and will be the subject of this presentation. Emphasis will be put on the National Security Agency (NSA) since it was and remains today the sole collector and processor of Communications Intelligence (COMINT, a form of SIGINT), the primary processor of Foreign Instrumentation Signals Intelligence (FISINT), and the coordinator of the US government’s national Electronics Intelligence (ELINT) program since 1958. Per se, the NSA is strictly a collection agency which means that it does not produce finished intelligence reports; this is the responsibility of NSA’s consumers within the US intelligence community.

From the Cold War to the 1990s

We still know very little about Cold War signals intelligence and even less about the role played by the NSA during the period from 1952 to the present. But the information now available leads us to conclude that SIGINT has been of vital importance during these years mainly because it succeeded where other intelligence sources failed. During the Cold War, the main objective was to discover what was going on behind the Iron Curtain, making the Soviet Union the obvious prime target. Spies could hardly penetrate the sealed, tightly-guarded Soviet Bloc and therefore interception of communications appeared to be a solution to monitor, from a distance, what was going on within the borders of the Soviet Union.

The NSA was born on 24 October 1952 when President Harry S. Truman signed a Top Secret eight-page directive entitled ‘Communications Intelligence Activities’, which made COMINT a national responsibility, and directed that all American COMINT activities ‘must be organized and managed as to exploit to the maximum the available resources of all participating departments and agencies and to satisfy the legitimate intelligence requirements of all such departments and agencies.’ The directive abolished the Armed Forces Security Agency (AFSA) and transferred all of its responsibilities and resources to the newly created National Security Agency based at Fort Meade, Maryland.

The 1950s were years of learning for the new agency and although it could count on the sympathy that President Dwight D. Eisenhower had for COMINT, it was a slow and painful learning process. However, by 1959, the NSA analysts had become more competent and more efficient in solving high-level Soviet cryptographic systems. The NSA reached the peak of its power during the 1960s mainly because of the demands of the Vietnam War, the collapse of spy networks in the Soviet Union, and the limitations on the use of imagery intelligence (IMINT). The NSA played an important role in the Cuban Missile Crisis of 1962, broke high-level Soviet as well as East German codes, followed Soviet Anti-Ballistic Missile (ABM) activities, and added satellite imagery to its array of intelligence sources.

The advent of microelectronics and new computer-based encryption technologies in the 1970s put the message senders ahead of the interceptors. But the NSA, despite budget and personnel cuts following the end of the Vietnam War, came to truly dominate the US intelligence community. The 1980s saw a massive growth of the NSA. In face of the dramatic increase in worldwide telecommunications traffic volumes, the NSA had to adapt and started to develop technologies which were and still are far ahead of those of any other nation in the world.

The interception of communications was the only reliable source of intelligence on Cold War Soviet Union and Eastern Europe, the so-called 'denied areas'. Geographic impediments and more global intelligence needs led to the creation of the UK-USA Communications Intelligence Agreement which organized the division of COMINT effort by the parties to the agreement against the Soviet Union and its communist allies. The vast majority of NSA's collection resources were devoted to monitoring the Soviet Union but the Americans, along with their British allies, were also reading the diplomatic traffic of dozens of other countries.

The Foreign Intelligence Surveillance Act

The NSA had always insisted to say that its power to eavesdrop came under no earthly laws but rather emanated from some celestial inherent presidential authority reposed in the chief executive by the Constitution. But on 23 March 1976, in the wake of the Watergate and the far-ranging intelligence abuses uncovered by the Church and Pike Committees, President Gerald R. Ford gave his blessings to a Senate bill that would have eliminated much of that inherent authority and, for the first time, required the NSA to submit to judicial review before initiating certain surveillances. After two unsuccessful attempts to get the bill passed in 1976 and in 1977, the Foreign Intelligence Surveillance Act (FISA) was finally signed into law by President Jimmy Carter on 25 October 1978.

The statute was aimed at bringing under the rule of law the electronic eavesdropping activities within the United States on foreign embassies, diplomats, and agents of foreign powers. The act established the Foreign Intelligence Surveillance Court with the task of granting or refusing surveillance warrants requested by the NSA or the FBI. In front of that 'court' which sits in secret session, holds no adversary hearings, and issues almost no public opinions or reports, the federal government never lost a case. In the court's first 15 months, ending in December 1980, it approved all 518 applications. Further analysis of the warrant process and of the FISA is provided in Bamford's book *Puzzle Palace* and concludes that the court has become a simple, procedural rubber stamp.

The UKUSA network of allies

The interception of communications for the protection of US national security is the task of the NSA but that task is also performed, indirectly, by its network of UKUSA allies. Soon after its creation, the NSA started to build intercept stations in the United States and around the world. Indeed, between 1950 and 1960, the NSA constructed at a cost of hundreds of millions of dollars a multi-layered network of 70 strategic intercept stations and an equal number of tactical COMINT units around the world. This network of American SIGINT intercept stations, together with the 35 or so radio intercept stations operated by Britain, Canada, Australia and New Zealand, stretched completely around the periphery of the Soviet Union, Eastern Europe, the People's Republic of China and North Korea, and was able to copy all important shortwave radio traffic coming from inside these countries.

Add to this mix the not inconsiderable SIGINT collection resources of NSA's Third Party partners in Norway, Denmark, West Germany, Austria, Italy, Greece, Turkey, Pakistan, Thailand, Nationalist China, Japan, and South Korea, and one can make the argument that the UKUSA partners possessed the largest and geographically best situated SIGINT collection system in the world, even if the Soviet SIGINT system was larger in terms of personnel.

Intercepting communications today: ECHELON

In the greatest surveillance effort ever established, the NSA has created a global surveillance system, codename ECHELON, which captures and analyzes virtually every phone call, fax, email and telex message sent anywhere in the world. ECHELON is controlled by the NSA and is operated in conjunction with the Second Parties to the UKUSA agreement: the British Government Communications Headquarters (GCHQ), the Canadian Communications Security Establishment (CSE), the Australian Defence Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand.

The ECHELON system is fairly simple in design. It is made of intercept stations all over the world capturing all satellite, microwave, cellular and fibre-optic communications traffic. This information is then processed through the massive computer capabilities of the NSA, which include advanced voice recognition and optical character recognition (OCR) programs. These computers look for code words or phrases (known as the ECHELON 'Dictionary') that will prompt them 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.

While signals intelligence technology was helpful in containing and eventually defeating the Soviet Empire during the Cold War, what was once designed to target a select list of communist countries and terrorist states is now indiscriminately directed against virtually every citizen in the world. The European Parliament is now asking whether the ECHELON communications interceptions violate the sovereignty and privacy of citizens in other countries. In some cases, such as the NSA's Menwith Hill station in England, surveillance is conducted against citizens on their own soil and with the full knowledge and cooperation of their government.

Conclusion

COMINT has shadowed the development of extensive high capacity new civil telecommunications systems, and has in consequence become a large-scale industrial activity employing many skilled workers and utilising exceptionally high degrees of automation. The targets of COMINT operations are varied. The most traditional COMINT targets are military messages and diplomatic communications between national capitals and missions abroad. Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of COMINT. More recent targets include narcotics trafficking, money laundering, terrorism and organised crime. But despite NSA's massive contribution to the protection of American national security, ordinary citizens and businesses have legitimate reasons to worry about the potential use of these tremendous capabilities for other purposes.

THE INTERCEPTION OF COMMUNICATIONS

Jérôme Mellon

30 April 2002

Bibliography

Matthew M. Aid, 'The National Security Agency and the Cold War', *Intelligence and National Security*, vol. 16, no. 1, January 2001, pp. 27-66.

Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*, London, HaperCollins, 1996.

James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency*, Boston, Houghton Mifflin, 1982.

Patrick S. Poole, 'ECHELON: America' s Secret Global Surveillance Network', *Patrick S. Poole' s Homepage*[Online], <http://fly.hiwaay.net/~pspoole/echelon.html> (Page visited on 24 February 2002).

On the Internet

The Foreign Intelligence Surveillance Act is Chapter 36 of Title 50 (War and National Defense) of the US Code. It is available on the Internet site of the Legal Information Institute, Cornell Law School at the following address:

<http://www4.law.cornell.edu/uscode/50/ch36.html>

Visit the Internet site of the Temporary committee on the ECHELON interception system of the European Parliament at the following address:

http://www.europarl.eu.int/committees/echelon_home.htm

The volume 2 of the report on Development of surveillance technology and risk of abuse of economic information, presented to the Director General for Research of the European Parliament and called Interception Capabilities 2000, is available at the following address:

http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm



An Agency of the United States
Department of Commerce

(1 of 1)

United States Patent
Nelson , et al.

5,937,422
August 10, 1999

Automatically generating a topic description for text and searching and sorting text by topic using the same

Abstract

A method of automatically generating a topical description of text by receiving the text containing input words; stemming each input word to its root form; assigning a user-definable part-of-speech score to each input word; assigning a language salience score to each input word; assigning an input-word score to each input word; creating a tree structure under each input word, where each tree structure contains the definition of the corresponding input word; assigning a definition-word score to each definition word; collapsing each tree structure to a corresponding tree-word list; assigning a tree-word-list score to each entry in each tree-word list; combining the tree-word lists into a final word list; assigning each word in the final word list a final-word-list score; and choosing the top N scoring words in the final word list as the topic description of the input text. Document searching and sorting may be accomplished by performing the method described above on each document in a database and then comparing the similarity of the resulting topical descriptions.

Inventors: **Nelson; Douglas J.** (Columbia, MD); **Schone; Patrick John** (Elkridge, MD);
Bates; Richard Michael (Greenbelt, MD)

Assignee: **The United States of America as represented by the National Security**
(Washington, DC)

Appl. No.: **834263**

Filed: **April 15, 1997**

Current U.S. Class

707/531; 707/4; 707/512; 707/532; 707/535

Intern'l Class:

G06F 017/30

Field of Search:

704/10 707/512,532,535,531,3-5,7
