DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

Vol 2/5

The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition

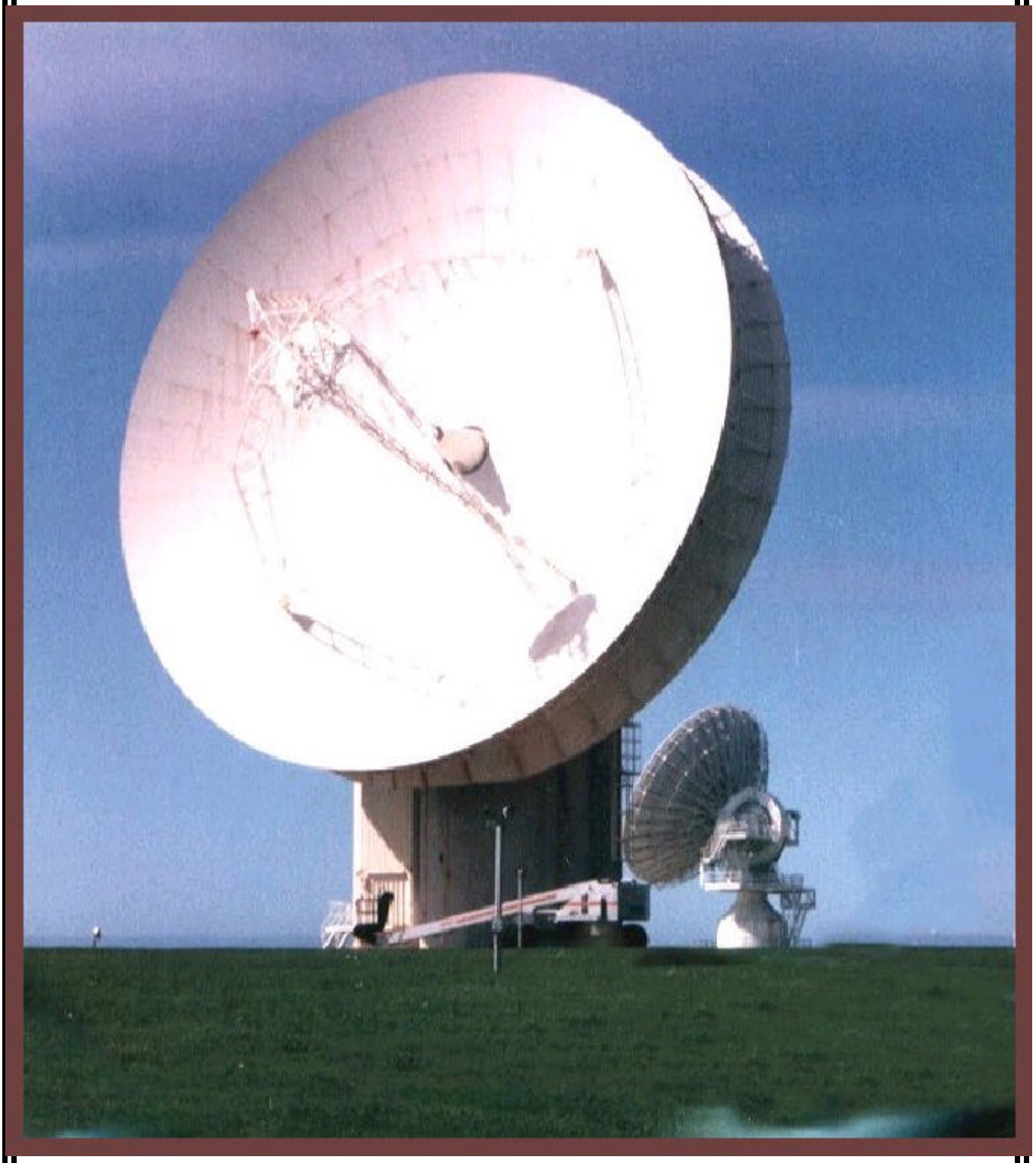
Working document for the STOA Panel

Luxembourg,October 1999 PE 168.184/Vol 2/5

Cataloguing data:

Title:	**Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ulti-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition**
Workplan Ref.:	EP/IV/B/STOA/98/1401
Publisher:	European Parliament Directorate General for Research Directorate A The STOA Programme
Author:	Duncan Campbell - IPTV Ltd.- Edinburgh
Editor:	Mr Dick HOLDSWORTH, Head of STOA Unit
Date:	October 1999
PE number:	**PE 168. 184 Vol 2/5**

Interception Capabilities 2000



Report to the Director General for Research of the European Parliament (Scientific and Technical Options Assessment programme office) on the development of surveillance technology and risk of abuse of

economic information. This study considers the state of the art in Communications intelligence (Comint) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to Comint targeting and selection, including speech recognition.

Interception Capabilities 2000

Contents

Duncan Campbell
IPTV Ltd
Edinburgh, Scotland
April, 1999

mailto:iptv@cwcom.net

Cover : 30 metre antennae at the Composite Signals Organisation Station, Morwenstow, England, intercepting communications from Atlantic Ocean and Indian Ocean regional satellites. (D Campbell)

Summary

1. **Communications intelligence** (Comint) involving the covert interception of foreign communications has been practised by almost every advanced nation since international telecommunications became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments. The capabilities of and constraints on Comint activity may usefully be considered in the framework of the "intelligence cycle" (section 1).

2. Globally, about 15-20 billion Euro is expended annually on Comint and related activities. The largest component of this expenditure is incurred by the major English-speaking nations of the UKUSA alliance. [1] This report describes how Comint organisations have for more than 80 years made arrangements to obtain access to much of the world's international communications. These include the unauthorised interception of commercial satellites, of long distance communications from space, of undersea cables using submarines, and of the Internet. In excess of 120 currently in simultaneous operation collecting intelligence (section 2).

3. The highly automated UKUSA system for processing Comint, often known as ECHELON, has been widely discussed within Europe following a 1997 STOA report.[2] That report summarised information from the only two primary sources then available on ECHELON. [3] This report provides original new documentary and other evidence about the ECHELON system and its involvement in the interception of communication satellites (section 3). A technical annexe give a supplementary, detailed description of Comint processing methods.

4. Comint information derived from the interception of international communications has long been routinely used to obtain sensitive data concerning individuals, governments, trade and international organisations. This report sets out the organisational and reporting frameworks within which economically sensitive information is collected and disseminated, summarising examples where European commercial organisations have been the subject of surveillance (section 4).

5. This report identifies a previously unknown international organisation - “ILETS” - which has, without parliamentary or public discussion or awareness, put in place contentious plans to require manufacturers and operators of new communications systems to build in monitoring capacity for use by national security or law enforcement organisations (section 5).

6. Comint organisations now perceive that the technical difficulties of collecting communications are increasing, and that future production may be costlier and more limited than at present. The perception of such difficulties may provide a useful basis for policy options aimed at protective measures concerning economic information and effective encryption (section 6).

7. **Key findings** concerning the state of the art in Comint include :

   - Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions (section 2, technical annexe);
   - Contrary to reports in the press, effective "word spotting" search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research. However, speaker recognition systems – in effect, "voiceprints" – have been developed and are deployed to recognise the speech of targeted individuals making international telephone calls;
   - Recent diplomatic initiatives by the United States government seeking European agreement to the "key escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-US nationals, including European governments, companies and citizens;
   - There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade.

1. Organisations and methods

What is communications intelligence?

1. Communications intelligence (Comint) is defined by NSA, the largest agency conducting such operations as "technical and intelligence information derived from foreign communications by other than their intended recipient". [4] Comint is a major component of Sigint (signals intelligence), which also includes the collection of non-communications signals, such as radar emissions.[5] Although this report deals with agencies and systems whose overall task may be Sigint, it is concerned only with Comint.

2. 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.

3. 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.

4. Whenever access to international communications channels is obtained for one purpose, access to every other type of communications carried on the same channels is automatic, subject only to the tasking requirements of agencies. Thus, for example, NSA and its British counterpart GCHQ, used Comint collected primarily for other purposes to provide data about domestic political opposition figures in the United States between 1967 and 1975.

UKUSA alliance

5. The United States Sigint System (USSS) consists of the National Security Agency (NSA), military support units collectively called the Central Security Service, and parts of the CIA and other organisations. Following wartime collaboration, in 1947 the UK and the US made a secret agreement to continue to conduct collaborative global Comint activities. Three other English-speaking nations, Canada, Australia and New Zealand joined the UKUSA agreement as "Second Parties". The UKUSA agreement was not acknowledged publicly until March 1999, when the Australian government confirmed that its Sigint organisation, Defence Signals Directorate (DSD) "does co-operate with counterpart signals intelligence organisations overseas under the UKUSA relationship".[6] The UKUSA agreement shares facilities, tasks and product between participating governments.

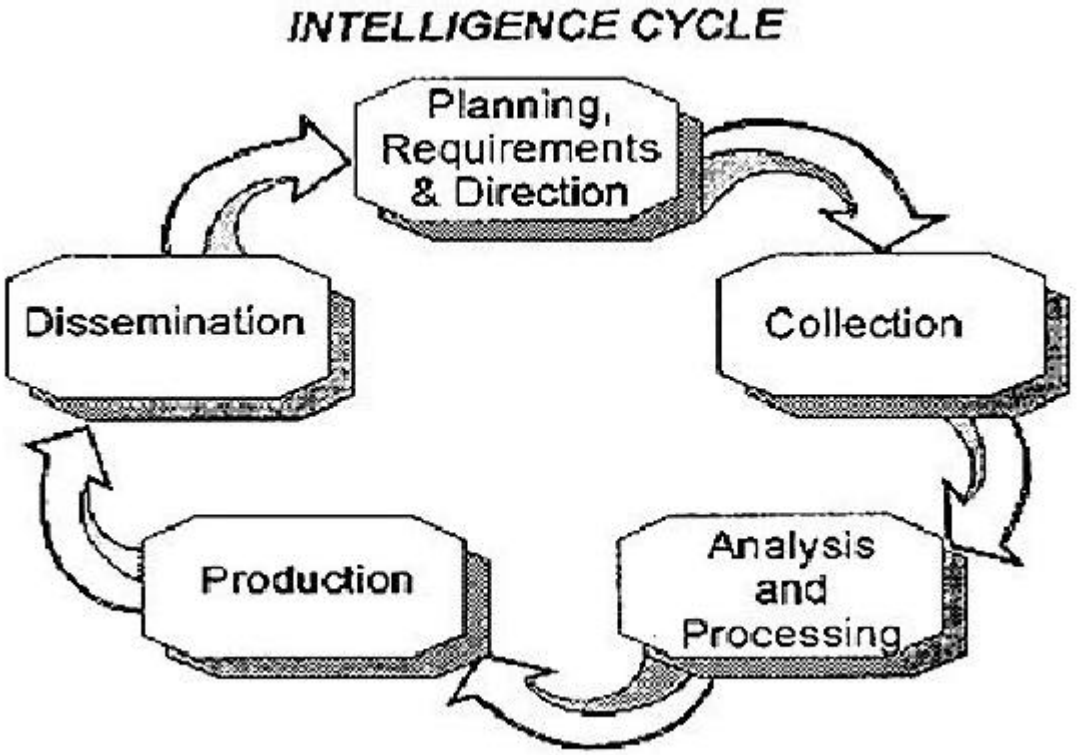
6. Although UKUSA Comint agency staffs and budgets have shrunk following the end of the cold war, they have reaffirmed their requirements for access to all the world's communications. Addressing NSA staff on his departure in 1992, then NSA director Admiral William Studeman described how "the demands for increased global access are growing". The "business area" of "global access" was, he said, one of "two, hopefully strong, legs upon which NSA must stand" in the next century.[7]

Other Comint organisations

7. Besides UKUSA, there at least 30 other nations operating major Comint organisations. The largest is the Russian FAPSI, with 54,000 employees.[8] China maintains a substantial Sigint system, two stations of which are directed at Russia and operate in collaboration with the United States. Most Middle Eastern and Asian nations have invested substantially in Sigint, in particular Israel, India and Pakistan.

How intelligence works

8. In the post cold war era, Comint interception has been constrained by recognisable industrial features, including the requirement to match budgets and capabilities to customer requirements. The multi-step process by means of which communications intelligence is sought, collected, processed and passed on is similar for all countries, and is often described as the "intelligence cycle". The steps of the intelligence cycle correspond to distinct organisational and technical features of Comint production. Thus, for example, the administration of NSA's largest field station in the world, at Menwith Hill in England and responsible for operating over 250



classified projects, is divided into three directorates: OP, Operations and Plans; CP, Collection Processing; and EP, Exploitation and Production.

Planning

9. Planning first involves determining customer requirements. Customers include the major ministries of the sponsoring government – notably those concerned with defence, foreign affairs, security, trade and home affairs. The overall management of Comint involves the identification of requirements for data as well as translating requirements into potentially achievable tasks, prioritising, arranging analysis and reporting, and monitoring the quality of Comint product.

10. Once targets have been selected, specific existing or new collection capabilities may be **tasked**, based on the type of information required, the susceptibility of the targeted activity to collection, and the likely effectiveness of collection.

Access and collection

11. The first essential of Comint is **access** to the desired communications medium so that communications may be intercepted. Historically, where long-range radio communications were used, this task was simple. Some important modern communications systems are not "Comint friendly" and may require unusual, expensive or intrusive methods to gain access. The physical means of communication is usually independent of the type of information carried. For example, inter-city microwave radio-relay systems, international satellite links and fibre optic submarine cables will all usually carry mixed traffic of television, telephone, fax, data links, private voice, video and data.

12. **Collection** follows **interception**, but is a distinct activity in that many types of signals may be intercepted but will receive no further processing save perhaps technical searches to verify that communications patterns remain unchanged. For example, a satellite interception station tasked to study a newly launched communications satellite will set up an antenna to intercept all that the satellite sends to the ground. Once a survey has established which parts of the satellite's signals carry, say, television or communications of no interest, these signals will not progress further within the system.

13. Collection includes both acquiring information by interception and passing information of interest downstream for **processing** and **production**. Because of the high information rates used in many modern networks, and the complexity of the signals within them, it is now common for high speed recorders or "snapshot" memories temporarily to hold large quantities of data while processing takes place. Modern collection activities use secure, rapid communications to pass data via global networks to human analysts who may be a continent

away. Selecting messages for collection and processing is in most cases automated, involving large on-line databanks holding information about targets of interest.

Processing

14. **Processing** is the conversion of collected information into a form suitable for analysis or the production of intelligence, either automatically or under human supervision. Incoming communications are normally converted into standard formats identifying their technical characteristics, together with message (or signal) related information (such as the telephone numbers of the parties to a telephone conversation).

15. At an early stage, if it is not inherent in the selection of the message or conversation, each intercepted signal or channel will be described in standard "case notation". Case notation first identifies the countries whose communications have been intercepted, usually by two letters. A third letter designates the general class of communications: C for commercial carrier intercepts, D for diplomatic messages, P for police channels, etc. A fourth letter designates the type of communications system (such as S for multi-channel). Numbers then designate particular links or networks. Thus for example, during the 1980s NSA intercepted and processed traffic designated as "FRD" (French diplomatic) from Chicksands, England, while the British Comint agency GCHQ deciphered "ITD" (Italian diplomatic) messages at its Cheltenham headquarters. [9]

16. Processing may also involve translation or "gisting" (replacing a verbatim text with the sense or main points of a communication). Translation and gisting can to some degree be automated.

Production and dissemination

17. Comint **production** involves analysis, evaluation, translation and interpretation of raw data into finished intelligence. The final step of the intelligence cycle is **dissemination**, meaning the passing of reports to the intelligence consumers. Such reports can consist of raw (but decrypted and/or translated) messages, gists, commentary, or extensive analyses. The quality and relevance of the disseminated reports lead in turn to the re-specification of intelligence collection priorities, thereby completing the intelligence cycle.

18. The nature of dissemination is highly significant to questions of how Comint is exploited to obtain economic advantage. Comint activities everywhere are highly classified because, it is argued, knowledge of the success of interception would be likely to lead targets to change their communications methods to defeat future interception. Within the UKUSA system, the dissemination of Comint reports is limited to individuals holding high-level security "SCI" clearances.[10] Further, because only cleared officials can see Comint reports, only they can set requirements and thus control tasking. Officials of commercial companies normally neither have clearance nor routine access to Comint, and may therefore only benefit from commercially relevant Comint information to the extent that senior, cleared government officials permit. The ways in which this takes place is described in Section 5, below.

19. Dissemination is further restricted within the UKUSA organisation by national and international rules generally stipulating that the Sigint agencies of each nation may not normally collect or (if inadvertently collected) record or disseminate information about citizens of, or companies registered in, any other UKUSA nation. Citizens and companies are collectively known as "legal persons". The opposite procedure is followed if the person concerned has been targeted by their national Comint organisation.

20. For example, Hager has described [11] how New Zealand officials were instructed to remove the names of identifiable UKUSA citizens or companies from their reports, inserting instead words such as "a Canadian citizen" or "a US company". British Comint staff have described following similar procedures in respect of US citizens following the introduction of legislation to limit NSA's domestic intelligence activities in 1978. [12]The Australian government says that "DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others … the Rules [on Sigint and Australian persons] prohibit the dissemination of information relating to Australian persons gained accidentally during the course of routine collection of foreign communications; or the reporting or recording of the names of Australian persons mentioned in foreign communications".[13] The corollary is also true; <u>UKUSA nations place no restrictions on intelligence gathering affecting either citizens or companies of any non-UKUSA nation, including member states of the European Union (except the UK)</u>.

2. Intercepting international communications

International Leased Carrier (ILC) communications

21. It is a matter of record that foreign communications to and from, or passing through the United Kingdom and the United States have been intercepted for more than 80 years.[14] Then and since, most international communications links have been operated by international carriers, who are usually individual national PTTs or private companies. In either case, capacity on the communication system is leased to individual national or international telecommunications undertakings. For this reason, Comint organisations use the term ILC (International Leased Carrier) to describe such collection.

High frequency radio

22. Save for direct landline connections between geographically contiguous nations, high frequency (HF) radio system were the most common means of international telecommunications prior to 1960, and were in use for ILC, diplomatic and military purposes. An important characteristic of HF radio signals is that they are reflected from the ionosphere and from the earth's surface, providing ranges of thousands of miles. This enables both reception and interception.

Microwave radio relay

23. Microwave radio was introduced in the 1950s to provide high capacity inter-city communications for telephony, telegraphy and, later, television. Microwave radio relay communications utilise low power transmitters and parabolic dish antennae placed on towers in high positions such as on hilltops or tall buildings. The antennae are usually 1-3m in diameter. Because of the curvature of the earth, relay stations are generally required every 30-50km.

Subsea cables

24. Submarine telephone cables provided the first major reliable high capacity international communications systems. Early systems were limited to a few hundred simultaneous telephone channels. The most modern optical fibre systems carry up to 5 Gbps (Gigabits per second) of digital information. This is broadly equivalent to about 60,000 simultaneous telephone channels.

Communications satellites

25. Microwave radio signals are not reflected from the ionosphere and pass directly into space. This property has been exploited both to provide global communications and, conversely, to intercept such communications in space and on land. The largest constellation of communications satellites (COMSATs) is operated by the International Telecommunications Satellite organisation (Intelsat), an international treaty organisation. To provide permanent communications from point to point or for broadcasting purposes, communications satellites are placed into so-called "geostationary" orbits such that, to the earth-based observer, they appear to maintain the same position in the sky.

26. The first geostationary Intelsat satellites were orbited in 1967. Satellite technology developed rapidly. The fourth generation of Intelsat satellites, introduced in 1971, provided capacity for 4,000 simulataneous telephone channels and were capable of handling all forms of communications simultaneously –telephone, telex, telegraph, television, data and facsimile. In 1999, Intelsat operated 19 satellites of its 5th to 8th generations. The latest generation can handle the equivalent to 90,000 simultaneous calls.

Communications techniques

27. Prior to 1970, most communications systems (however carried) utilised analogue or continuous wave techniques. Since 1990, almost all communications have been digital, and are providing ever higher capacity. The highest capacity systems in general use for the Internet, called STM-1 or OC-3, operates at a data rate of 155Mbs. (Million bits per second; a rate of 155 Mbps is equivalent to sending 3 million words every second, roughly the text of one thousand books a minute.) For example, links at this capacity are used to provide backbone Internet connections between Europe and the United States. Further details of communications techniques are given in the technical annexe.

ILC communications collection

Access

28. Comint collection cannot take place unless the collecting agency obtains access to the communications channels they wish to examine. Information about the means used to gain access are, like data about code-breaking methods, the most highly protected information within any Comint organisation. Access is gained both with and without the complicity or co-operation of network operators.

Operation SHAMROCK

29. From 1945 onwards in the United States the NSA and predecessor agencies systematically obtained cable traffic from the offices of the major cable companies. This activity was codenamed SHAMROCK. These activities remained unknown for 30 years, until enquiries were prompted by the Watergate affair. On 8 August 1975, NSA Director Lt General Lew Allen admitted to the Pike Committee of the US House of Representatives that :

"NSA systematically intercepts international communications, both voice and cable".

High frequency radio interception antenna (AN/FLR9)

DOJOCC sign at NSA Station, Chicksands.

30. He also admitted that "messages to and from American citizens have been picked up in the course of gathering foreign intelligence". US legislators considered that such operations might have been unconstitutional. During 1976, a Department of Justice team investigated possible criminal offences by NSA. Part of their report was released in 1980. It described how intelligence on US citizens:

> *"was obtained <u>incidentally</u> in the course of NSA's interception of aural and non-aural (e.g., telex) international communications and the receipt of GCHQ-acquired telex and ILC (International Leased Carrier) cable traffic (SHAMROCK)" (emphasis in original).* [15]

High frequency radio interception

31. High frequency radio signals are relatively easy to intercept, requiring only a suitable area of land in, ideally, a "quiet" radio environment. From 1945 until the early 1980s, both NSA and GCHQ operated HF radio interception systems tasked to collect European ILC communications in Scotland. [16]

32. The most advanced type of HF monitoring system deployed during this period for Comint purposes was a large circular antenna array known as AN/FLR-9. AN/FLR-9 antennae are more than 400 metres in diameter. They can simultaneously intercept and determine the bearing of signals from as many directions and on as many frequencies as may be desired. In 1964, AN/FLR-9 receiving systems were installed at San Vito dei Normanni, Italy; Chicksands, England, and Karamursel, Turkey.

33. In August 1966, NSA transferred ILC collection activities from its Scottish site at Kirknewton, to Menwith Hill in England. Ten years later, this activity was again transferred, to Chicksands. Although the primary function of the Chicksands site was to intercept Soviet and Warsaw Pact air force communications, it was also tasked to collect ILC and "NDC" (Non-US Diplomatic Communications). Prominent among such tasks was the collection of FRD traffic (i.e., French diplomatic communications). Although most personnel at Chicksands were members of the US Air Force, diplomatic and ILC interception was handled by civilian NSA employees in a unit called DODJOCC. [17]

34. During the 1970s, British Comint units on Cyprus were tasked to collect HF communications of allied NATO nations, including Greece and Turkey. The interception took place at a British army unit at Ayios Nikolaos, eastern Cyprus.[18] In the United States in 1975, investigations by a US Congressional Committee revealed that NSA was collecting diplomatic messages sent to and from Washington from an army Comint site at Vint Hill Farms, Virginia. The targets of this station included the United Kingdom.[19]

Inter-city microwave radio relay tower "spills" its signals into space (below)

Space interception of inter-city networks

35. Long distance microwave radio relay links may require dozens of intermediate stations to receive and re-transmit communications. Each subsequent receiving station picks up only a tiny fraction of the original transmitted signal; the remainder passes over the horizon and on into space, where satellites can collect it. These principles were exploited during the 1960s to provide Comint collection from space. The nature of microwave "spillage" means that the best position for such satellites is not above the chosen target, but up to 80 degrees of longitude away.

36. The first US Comint satellite, CANYON, was launched In August 1968, followed soon by a second. The satellites were controlled from a ground station at Bad Aibling, Germany. In order to provide permanent coverage of selected targets, CANYON satellites were placed close to geostationary orbits. However, the orbits were not exact, causing the satellites to change position and obtain more data on ground targets.[20] Seven CANYON satellites were launched between 1968 and 1977.

links extended for thousands of miles, much of it over Siberia, where permafrost restricted the reliable use of underground cables. Geographical circumstances thus favoured NSA by making Soviet internal communications links highly accessible. The satellites performed better than expected, so the project was extended.

38. The success of CANYON led to the design and deployment of a new class of Comint satellites, CHALET. The ground station chosen for the CHALET series was Menwith Hill, England. Under NSA project P-285, US companies were contracted to install and assist in operating the satellite control system and downlinks (RUNWAY) and ground processing system (SILKWORTH). The first two CHALET satellites were launched in June 1978 and October 1979. After the name of the first satellite appeared in the US press, they were renamed VORTEX. In 1982, NSA obtained approval for expanded "new mission requirements" and were given funds and facilities to operate four VORTEX satellites simultaneously. A new 5,000m^2 operations centre (STEEPLEBUSH) was constructed to house processing equipment. When the name VORTEX was published in 1987, the satellites were renamed MERCURY.[21]

39. The expanded mission given to Menwith Hill after 1985 included MERCURY collection from the Middle East. The station received an award for support to US naval operations in the Persian Gulf from 1987 to 1988. In 1991, a further award was given for support of the Iraqi war operations, Desert Storm and Desert Shield.[22] Menwith Hill is now the major US site for Comint collection against its major ally, Israel. Its staff includes linguists trained in Hebrew, Arabic and Farsi as well as European languages. Menwith Hill has recently been expanded to include ground links for a new network of Sigint satellites launched in 1994 and 1995 (RUTLEY). The name of the new class of satellites remains unknown.

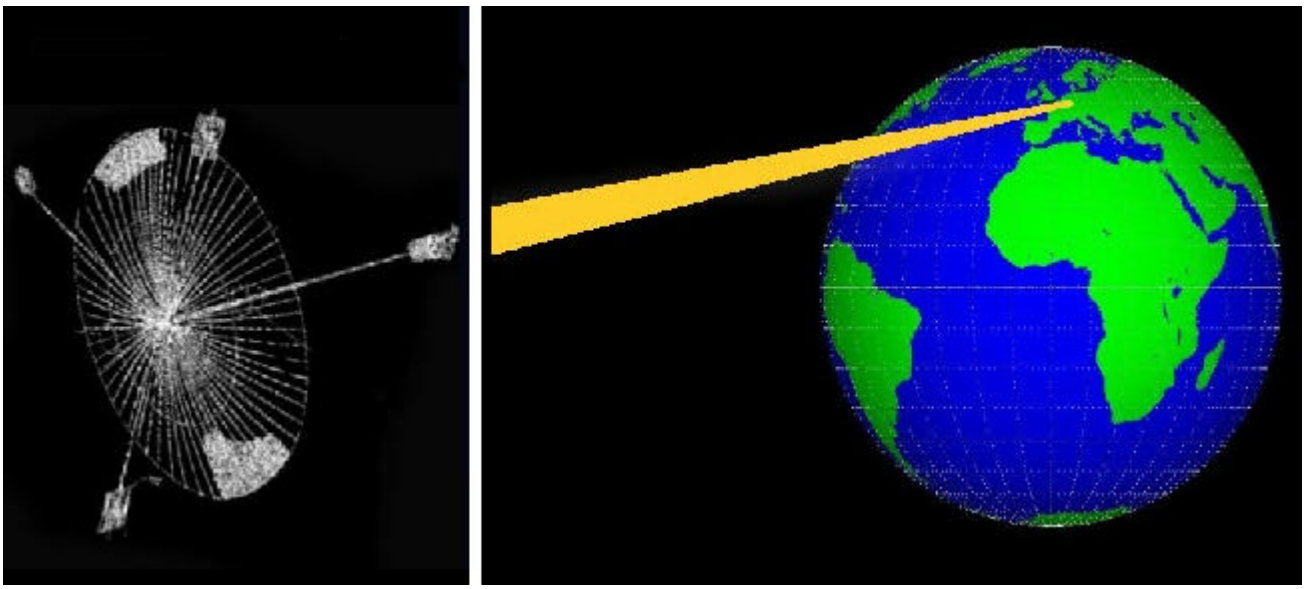
Sigint satellites

40. The CIA developed a second class of Sigint satellite with complementary capabilities over the period from 1967 to 1985. Initially known as RHYOLITE and later AQUACADE, these satellites were operated from a remote ground station in central Australia, Pine Gap. Using a large parabolic antenna which unfolded in space, RHYOLITE intercepted lower frequency signals in the VHF and UHF bands. Larger, most recent satellites of this type have been named MAGNUM and then ORION. Their targets include telemetry, VHF radio, cellular mobile phones, paging signals, and mobile data links.

41. A third class of satellite, known first as JUMPSEAT and latterly as TRUMPET, operates in highly elliptical near-polar orbits enabling them to "hover" for long period over high northern latitudes. They enable the United States to collect signals from transmitters in high northern latitudes poorly covered by MERCURY or ORION, and also to intercept signals sent to Russian communications satellites in the same orbits.

42. Although precise details of US space-based Sigint satellites launched after 1990 remain obscure, it is apparent from observation of the relevant ground centres that collection systems have expanded rather than contracted. The main stations are at Buckley Field, Denver, Colorado; Pine Gap, Australia; Menwith Hill, England; and Bad Aibling, Germany. The satellites and their processing facilities are exceptionally costly (of the order of $1 billion US each). In 1998, the US National Reconnaissance Office (NRO) announced plans to combine the three separate classes of Sigint satellites into an Integrated Overhead Sigint Architecture (IOSA) in order to " improve Sigint performance and avoid costs by consolidating systems, utilising … new satellite and data processing technologies". [23]

43. It follows that, within constraints imposed by budgetary limitation and tasking priorities, the United States can if it chooses direct space collection systems to intercept mobile communications signals and microwave city-to-city traffic anywhere on the planet. The geographical and processing difficulties of collecting messages simultaneously from all parts of the globe suggest strongly that the tasking of these satellites will be directed towards the highest priority national and military targets. Thus, although European communications passing on inter-city microwave routes can be collected, it is likely that they are normally ignored. But it is very highly probable that communications to or from Europe and which pass through the microwave communications networks of Middle Eastern states are collected and processed.



Comint satellites in geostarionary orbits, such as VORTEX, intercept terrestial microwave "spillage".

44. No other nation (including the former Soviet Union) has deployed satellites comparable to CANYON, RHYOLITE, or their successors. Both Britain (project ZIRCON) and France (project ZENON) have attempted to do so, but neither persevered. After 1988 the British government purchased capacity on the US VORTEX (now MERCURY) constellation to use for unilateral national purposes. [24] A senior UK Liaison Officer and staff from GCHQ work at Menwith Hill NSA station and assist in tasking and operating the satellites.

COMSAT ILC collection

45. Systematic collection of COMSAT ILC communications began in 1971. Two ground stations were built for this purpose. The first at Morwenstow, Cornwall, England had two 30-metre antennae. One intercepted communications from the Atlantic Ocean Intelsat; the other the Indian Ocean Intelsat. The second Intelsat interception site was at Yakima, Washington in the northwestern United States. NSA's "Yakima Research Station" intercepted communications passing through the Pacific Ocean Intelsat satellite.

46. ILC interception capability against western-run communications satellites remained at this level until the late 1970s, when a second US site at Sugar Grove, West Virginia was added to the network. By 1980, its three satellite antenna had been reassigned to the US Naval Security Group and were used for COMSAT interception. Large-scale expansion of the ILC satellite interception system took place between 1985 and 1995, in conjunction with the enlargement of the ECHELON processing system (section 3). New stations were constructed in the United States (Sabana Seca, Puerto Rico), Canada (Leitrim, Ontario), Australia (Kojarena, Western Australia) and New Zealand (Waihopai, South Island). Capacity at Yakima, Morwenstow and Sugar Grove was expanded, and continues to expand.

    Based on a simple count of the number of antennae currently installed at each COMSAT interception or satellite SIGINT station, it appears that indicates that **the UKUSA nations are between them currently operating at least 120 satellite based collection systems.** The approximate number of antennae in each category are :

    - **Tasked on western commercial communications satellites (ILC) 40**
    - **Controlling space based signals intelligence satellites 30**
    - **Currently or formerly tasked on Soviet communications satellites 50**

    Systems in the third category may have been reallocated to ILC tasks since the end of the cold war. [25]

47. Other nations increasingly collect Comint from satellites. Russia's FAPSI operates large ground collection sites at Lourdes, Cuba and at Cam Ranh Bay, Vietnam.[26] Germany's BND and France's DGSE are alleged to collaborate in the operation of a COMSAT collection site at Kourou, Guyana, targeted on "American and South American satellite communications". DGSE is also said to have COMSAT collection sites at Domme (Dordogne, France), in New Caledonia, and in the United Arab Emirates.[27] The Swiss intelligence service has recently announced a plan for two COMSAT interception stations.[28]

Satellite ground terminal at Etam, West Virginia, connecting Europe and the US via Intelsat IV

GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA

Submarine cable interception

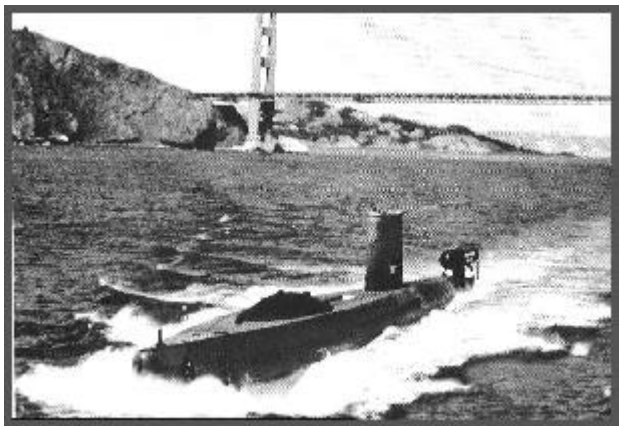
48. Submarine cables now play a dominant role in international telecommunications, since – in contrast to the limited bandwidth available for space systems – optical media offer seemingly unlimited capacity. Save where cables terminate in countries where telecommunications operators provide Comint access (such as the UK and the US), submarine cables appear intrinsically secure because of the nature of the ocean environment.

49. In October 1971, this security was shown not to exist. A US submarine, Halibut, visited the Sea of Okhotsk off the eastern USSR and recorded communications passing on a military cable to the Khamchatka Peninsula. Halibut was equipped with a deep diving chamber, fully in view on the submarine's stern. The chamber was described by the US Navy as a "deep submergence rescue vehicle". The truth was that the "rescue vehicle" was welded immovably to the submarine. Once submerged, deep-sea divers exited the submarine and wrapped tapping coils around the cable. Having proven the principle, USS Halibut returned in 1972 and laid a high capacity recording pod next to the cable. The technique involved no physical damage and was unlikely to have been readily detectable. [29]

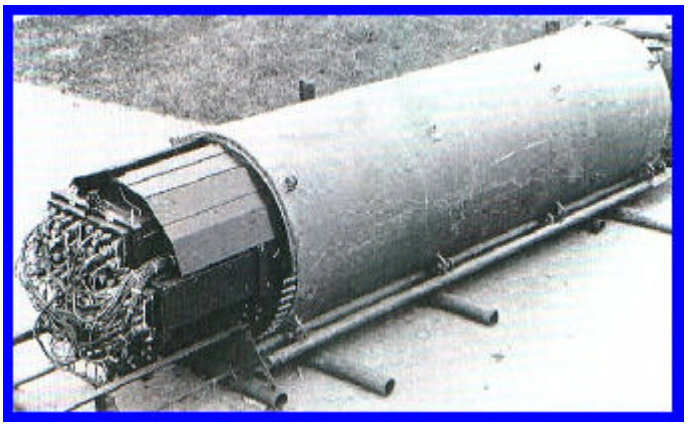
50. The Okhotsk cable tapping operation continued for ten years, involving routine trips by three different specially equipped submarines to collect old pods and lay new ones; sometimes, more than one pod at a time. New targets were added in 1979. That summer, a newly converted submarine called USS Parche travelled from San Francisco under the North Pole to the Barents Sea, and laid a new cable tap near Murmansk. Its crew received a presidential citation for their achievement. The Okhotsk cable tap ended in 1982, after its location was compromised by a former NSA employee who sold information about the tap, codenamed IVY BELLS, to the Soviet Union. One of the IVY BELLS pods is now on display in the Moscow museum of the former KGB. The cable tap in the Barents Sea continued in operation, undetected, until tapping stopped in 1992.

51. During 1985, cable-tapping operations were extended into the Mediterranean, to intercept cables linking Europe to West Africa. [30] After the cold war ended, the USS Parche was refitted with an extended section to accommodate larger cable tapping equipment and pods. Cable taps could be laid by remote control, using drones. USS Parche continues in operation to the present day, but the precise targets of its missions remain unknown. The Clinton administration evidently places high value on its achievements, Every year from 1994 to 1997, the submarine crew has been highly commended. [31] Likely targets may include the Middle East, Mediterranean, eastern Asia, and South America. The United States is the only naval power known to have deployed deep-sea technology for this purpose.

52. Miniaturised inductive taps recorders have also been used to intercept underground cables.[32] Optical fibre cables, however, do not leak radio frequency signals and cannot be tapped using inductive loops. NSA and other Comint agencies have spent a great deal of money on research into tapping optical fibres, reportedly with little success. But long distance optical fibre cables are not invulnerable. The key means of access is by tampering with optoelectronic "repeaters" which boost signal levels over long distances. It follows that any submarine cable system using submerged optoelectronic repeaters cannot be considered secure from



USS Halibut with disguised chamber for diving



Cable tapping pod laid by US submarine off Khamchatka

interception and communications intelligence activity.

Intercepting the Internet

53. The dramatic growth in the size and significance of the Internet and of related forms of digital communications has been argued by some to pose a challenge for Comint agencies. This does not appear correct. During the 1980s, NSA and its UKUSA partners operated a larger international communications network than the then Internet but based on the same technology.[33] According to its British partner "all GCHQ systems are linked together on the largest LAN [Local Area Network] in Europe, which is connected to other sites around the world via one of the largest WANs [Wide Area Networks] in the world … its main networking protocol is Internet Protocol (IP).[34] This global network, developed as project EMBROIDERY, includes PATHWAY, the NSA's main computer communications network. It provides fast, secure global communications for ECHELON and other systems.

54. Since the early 1990s, fast and sophisticated Comint systems have been developed to collect, filter and analyse the forms of fast digital communications used by the Internet. Because most of the world's Internet capacity lies within the United States or connects to the United States, many communications in "cyberspace" will pass through intermediate sites within the United States. Communications from Europe to and from Asia, Oceania, Africa or South America normally travel via the United States.

55. Routes taken by Internet "packets" depend on the origin and destination of the data, the systems through which they enter and leaves the Internet, and a myriad of other factors including time of day. Thus, routers within the western United States are at their most idle at the time when central European traffic is reaching peak usage. It is thus possible (and reasonable) for messages travelling a short distance in a busy European network to travel instead, for example, via Internet exchanges in California. It follows that a large proportion of international communications on the Internet will by the nature of the system pass through the United States and thus be readily accessible to NSA.

56. Standard Internet messages are composed of packets called "datagrams" . Datagrams include numbers representing both their origin and their destination, called "IP addresses". The addresses are unique to each computer connected to the Internet. They are inherently easy to identify as to country and site of origin and destination. Handling, sorting and routing millions of such packets each second is fundamental to the operation of major Internet centres. The same process facilitates extraction of traffic for Comint purposes.

57. Internet traffic can be accessed either from international communications links entering the United States, or when it reaches major Internet exchanges. Both methods have advantages. Access to communications systems is likely to be remain clandestine - whereas access to Internet exchanges might be more detectable

but provides easier access to more data and simpler sorting methods. Although the quantities of data involved are immense, NSA is normally legally restricted to looking only at communications that start or finish in a foreign country. Unless special warrants are issued, all other data should normally be thrown away by machine before it can be examined or recorded.

58. Much other Internet traffic (whether foreign to the US or not) is of trivial intelligence interest or can be handled in other ways. For example, messages sent to "Usenet" discussion groups amounts to about 15 Gigabytes (GB) of data per day; the rough equivalent of 10,000 books. All this data is broadcast to anyone wanting (or willing) to have it. Like other Internet users, intelligence agencies have open source access to this data and store and analyse it. In the UK, the Defence Evaluation and Research Agency maintains a 1 Terabyte database containing the previous 90 days of Usenet messages.[35] A similar service, called "Deja News", is available to users of the World Wide Web (WWW). Messages for Usenet are readily distinguishable. It is pointless to collect them clandestinely.

59. Similar considerations affect the World Wide Web, most of which is openly accessible. Web sites are examined continuously by "search engines" which generate catalogues of their contents. "Alta Vista" and "Hotbot" are prominent public sites of this kind. NSA similarly employs computer "bots" (robots) to collect data of interest. For example, a New York web site known as JYA.COM (http://www.jya.com/cryptome) offers extensive public information on Sigint, Comint and cryptography. The site is frequently updated. Records of access to the site show that every morning it is visited by a "bot" from NSA's National Computer Security Centre, which looks for new files and makes copies of any that it finds.[36]

60. It follows that foreign Internet traffic of communications intelligence interest – consisting of e-mail, file transfers, "virtual private networks" operated over the internet, and some other messages - will form at best a few per cent of the traffic on most US Internet exchanges or backbone links. According to a former employee, NSA had by 1995 installed “sniffer” software to collect such traffic at nine major Internet exchange points (IXPs).[37] The first two such sites identified, FIX East and FIX West, are operated by US government agencies. They are closely linked to nearby commercial locations, MAE East and MAE West (see table). Three other sites listed were Network Access Points originally developed by the US National Science Foundation to provide the US Internet with its initial "backbone".

Internet site	Location	Operator	Designation
FIX East	College Park, Maryland	US government	Federal Information Exchange
FIX West	Mountain View, California	US government	Federal Information Exchange
MAE East	Washington, DC	MCI	Metropolitan Area Ethernet
New York NAP	Pennsauken, New Jersey	Sprintlink	Network Access Point
SWAB	Washington, DC	PSInet / Bell Atlantic	SMDS Washington Area Bypass
Chicago NAP	Chicago, Illinois	Ameritech / Bellcorp	Network Access Point
San Francisco NAP	San Francisco, California	Pacific Bell	Network Access Point
MAE West	San Jose, California	MCI	Metropolitan Area Ethernet
CIX	Santa Clara California	CIX	Commercial Internet Exchange

Table 1 NSA Internet Comint access at IXP sites (1995) [38]

61. The same article alleged that a leading US Internet and telecommunications company had contracted with NSA to develop software to capture Internet data of interest, and that deals had been struck with the leading manufacturers Microsoft, Lotus, and Netscape to alter their products for foreign use. The latter allegation has proven correct (see technical annexe). Providing such features would make little sense unless NSA had also arranged general access to Internet traffic. Although NSA will not confirm or deny such allegations, a 1997 court case in Britain involving alleged "computer hacking" produced evidence of NSA surveillance of the Internet. Witnesses from the US Air Force component of NSA acknowledged using packet sniffers and specialised programmes to track attempts to enter US military computers. The case collapsed after the witnesses refused to provide evidence about the systems they had used.[39]

Covert collection of high capacity signals

62. Where access to signals of interest is not possible by other means, Comint agencies have constructed special purpose interception equipment to install in embassies or other diplomatic premises, or even to carry by hand to locations of special interest. Extensive descriptions of operations of this kind have been published by Mike

Frost, a former official of CSE, the Canadian Sigint agency.[40] Although city centre embassy premises are often ideally situated to intercept a wide range of communications, ranging from official carphone services to high capacity microwave links, processing and passing on such information may be difficult. Such collection operations are also highly sensitive for diplomatic reasons. Equipment for covert collection is therefore specialised, selective and miniaturised.

63. A joint NSA/CIA "Special Collection Service" manufactures equipment and trains personnel for covert collection activities One major device is a suitcase-sized computer processing system. ORATORY. ORATORY is in effect a miniaturised version of the Dictionary computers described in the next section, capable of selecting non-verbal communications of interest from a wide range of inputs, according to pre-programmed selection criteria. One major NSA supplier ("The IDEAS Operation") now offers micro-miniature digital receivers which can simultaneously process Sigint data from 8 independent channels. This radio receiver is the size of a credit card. It fits in a standard laptop computer. IDEAS claim, reasonably, that their tiny card "performs functions that would have taken a rack full of equipment not long ago".

New satellite networks

64. New network operators have constructed mobile phone systems providing unbroken global coverage using satellites in low or medium level earth orbits. These systems are sometimes called satellite personal communications systems (SPCS). Because each satellite covers only a small area and moves fast, large numbers of satellites are needed to provide continuous global coverage. The satellites can relay signals directly between themselves or to ground stations. The first such system to be completed, Iridium, uses 66 satellites and started operations in 1998. Iridium appears to have created particular difficulties for communications intelligence agencies, since the signals down from the Iridium and similar networks can only be received in a small area, which may be anywhere on the earth's surface.

3. ECHELON and Comint production

65. The ECHELON system became well known following publication of the previous STOA report. Since then, new evidence shows that ECHELON has existed since the 1970s, and was greatly enlarged between 1975 and 1995. Like ILC interception, ECHELON has developed from earlier methods. This section includes new information and documentary evidence about ECHELON and satellite interception.

The "Watch List"

66. After the public revelation of the SHAMROCK interception programme, NSA Director Lt General Lew Allen described how NSA used '"watch lists" as an aid to watch for foreign activity of reportable intelligence interest".[41] "We have been providing details … of any messages contained in the foreign communications we intercept that bear on named individuals or organisations. These compilations of names are commonly referred to as 'Watch Lists'", he said.[42] Until the 1970s, Watch List processing was manual. Analysts examined intercepted ILC communications, reporting, "gisting" or analysing those which appeared to cover names or topics on the Watch List.

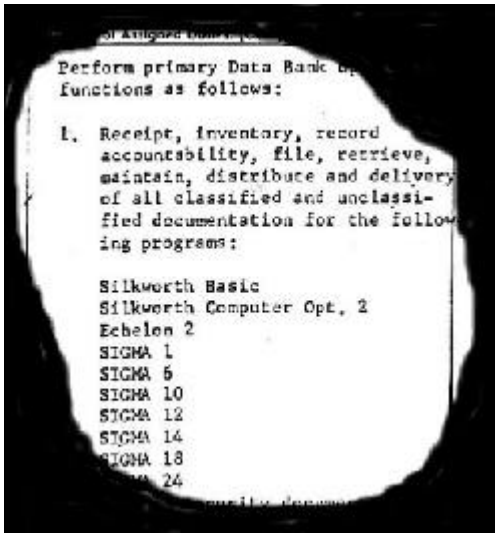
New information about ECHELON sites and systems

67. It now appears that the system identified as ECHELON has been in existence for more than 20 years. The need for such a system was foreseen in the late 1960s, when NSA and GCHQ planned ILC satellite interception stations at Mowenstow and Yakima. It was expected that the quantity of messages intercepted from the new satellites would be too great for individual examination. According to former NSA staff, the first ECHELON computers automated Comint processing at these sites.[43]

68. NSA and CIA then discovered that Sigint collection from space was more effective than had been anticipated, resulting in accumulations of recordings that outstripped the available supply of linguists and analysts. Documents show that when the SILKWORTH processing systems was installed at Menwith Hill for the new satellites, it was supported by ECHELON 2 and other databanks (see illustration).

69. By the mid 1980s, communications intercepted at these major stations were heavily sifted, with a wide variety of specifications available for non-verbal traffic. Extensive further automation was planned in the mid 1980s as NSA Project P-415. Implementation of this project completed the automation of the previous Watch List activity. From 1987 onwards, staff from international Comint agencies travelled to the US to attended training courses for the new computer systems.

70. Project P-415/ECHELON made heavy use of NSA and GCHQ's global Internet-like communication network to enable remote intelligence customers to task computers at each collection site, and receive the results automatically. The key component of the system are local "Dictionary" computers, which store an extensive database on specified targets, including names, topics of interest, addresses, telephone numbers and other selection criteria. Incoming messages are compared to these criteria; if a match is found, the raw intelligence is forwarded automatically. Dictionary computers are tasked with many thousands of different collection requirements, described as "numbers" (four digit codes).


Perform primary Data Bank
functions as follows:

1. Receipt, inventory, record accountability, file, retrieve, maintain, distribute and delivery of all classified and unclassified documentation for the following programs:

Silkworth Basic
Silkworth Computer Opt. 2
Echelon 2
SIGMA 1
SIGMA 6
SIGMA 10
SIGMA 12
SIGMA 14
SIGMA 18
24

List of intelligence databanks operating at Menwith Hill in 1979 included the second generation of ECHELON

ECHELON satellite interception site at Sugar Grove, West Virgina, showing 6 antenna targeted on European and Atlantic regional communications satellites (November 1998)

71. Tasking and receiving intelligence from the Dictionaries involves processes familiar to anyone who has used the Internet. Dictionary sorting and selection can be compared to using search engines, which select web pages containing key words or terms and specifying relationships. The forwarding function of the Dictionary computers may be compared to e-mail. When requested, the system will provide lists of communications matching each criterion for review, analysis, "gisting" or forwarding. An important point about the new system is that before ECHELON, different countries and different stations knew what was being intercepted and to whom it was sent. Now, all but a fraction of the messages selected by Dictionary computers at remote sites are forwarded to NSA or other customers without being read locally.

Westminster, London – Dictionary computer

72. In 1991, a British television programme reported on the operations of the Dictionary computer at GCHQ's Westminster, London office. The system "secretly intercepts every single telex which passes into, out of or through London; thousands of diplomatic, business and personal messages every day. These are fed into a programme known as `Dictionary'. It picks out keywords from the mass of Sigint, and hunts out hundreds of individuals and corporations".[44] The programme pointed out that the Dictionary computers, although controlled and tasked by GCHQ, were operated by security vetted staff employed by British Telecom (BT), Britain's dominant telecommunications operator.[45] The presence of Dictionary computers has also been confirmed at Kojarena, Australia; and at GCHQ Cheltenham, England.[46]

Sugar Grove, Virginia – COMSAT interception at ECHELON site

73. US government documents confirm that the satellite receiving station at Sugar Grove, West Virginia is an ECHELON site, and that collects intelligence from COMSATs. The station is about 250 miles south-west of Washington, in a remote area of the Shenandoah Mountains. It is operated by the US Naval Security Group and the US Air Force Intelligence Agency.

74. An upgraded system called TIMBERLINE II, was installed at Sugar Grove in the summer of 1990. At the same time, according to official US documents, an "ECHELON training department" was established. [47] With training complete, the task of the station in 1991 became "to **maintain and operate an ECHELON site**". [48]

75. The US Air Force has publicly identified the intelligence activity at Sugar Grove: its "mission is to **direct satellite communications equipment [in support of] consumers of COMSAT information** ... This is achieved by providing a trained cadre of collection system operators, analysts and managers". [49] In 1990, satellite photographs showed that there were 4 satellite antennae at Sugar Grove. By November 1998, ground inspection revealed that this had expanded to a group of 9.

Sabana Seca, Puerto Rico and Leitrim, Canada – COMSAT interception sites

76. Further information published by the US Air Force identifies the US Naval Security Group Station at Sabana Seca, Puerto Rico as a COMSAT interception site. Its mission is "to become the premier **satellite communications processing and analysis** field station". [50]

77. Canadian Defence Forces have published details about staff functions at the Leitrim field station of the Canadian Sigint agency CSE. The station, near Ottawa, Ontario has four satellite terminals, erected since 1984. The staff roster includes seven Communications Satellite Analysts, Supervisors and Instructors. [51]

78. In a publicly available resume, a former Communication Satellite Analyst employed at Leitrim describes his job as having required expertise in the "**operation and analysis of numerous Comsat computer systems and associated subsystems ... [utilising] computer assisted analysis systems ... [and] a broad range of sophisticated electronic equipment to intercept and study foreign communications and electronic transmissions**." [52] Financial reports from CSE also indicate that in 1995/96, the agency planned payments of $7 million to ECHELON and $6 million to Cray (computers). There were no further details about ECHELON. [53]

Waihopai, New Zealand – Intelsat interception at ECHELON site

79. New Zealand's Sigint agency GCSB operates two satellite interception terminals at Waihopai, tasked on Intelsat satellites covering the Pacific Ocean. Extensive details have already been published about the station's Dictionary computers and its role in the ECHELON network. [54] After the book was published, a New Zealand TV station obtained images of the inside of the station operations centre. The pictures were obtained clandestinely by filming through partially curtained windows at night. The TV reporter was able to film close-ups of technical manuals held in the control centre. These were **Intelsat technical manuals**, providing confirmation that the station targeted these satellites Strikingly, the station was seen to be virtually empty, operating fully automatically. One guard was inside, but was unaware he was being filmed. [55]

ILC processing techniques

80. The technical annexe describes the main systems used to extract and process communications intelligence. The detailed explanations given about processing methods are not essential to understanding the core of this report, but are provided so that readers knowledgeable about telecommunications may fully evaluate the state of the art.

81. Fax messages and computer data (from modems) are given priority in processing because of the ease with which they are understood and analysed. The main method of filtering and analysing non-verbal traffic, the Dictionary computers, utilise traditional information retrieval techniques, including keywords. Fast special purpose chips enable vast quantities of data to be processed in this way. The newest technique is "topic spotting". The processing of telephone calls is mainly limited to identifying call-related information, and traffic analysis. Effective voice "wordspotting" systems do not exist are not in use, despite reports to the contrary. But "voiceprint" type speaker identification systems have been in use since at least 1995. The use of strong cryptography is slowly impinging on Comint agencies' capabilities. This difficulty for Comint agencies has been offset by covert and overt activities which have subverted the effectiveness of cryptographic systems supplied from and/or used in Europe.

82. The conclusions drawn in the annexe are that Comint equipment currently available has the capability, as tasked, to intercept, process and analyse every modern type of high capacity communications system to which access is obtained, including the highest levels of the Internet. There are few gaps in coverage. The scale, capacity and speed of some systems is difficult fully to comprehend. Special purpose systems have been built to process pager messages, cellular mobile radio and new satellites.

4. Comint and Law Enforcement

83. In 1990 and 1991, the US government became concerned that the marketing of a secure telephone system by AT&T could curtail Comint activity. AT&T was persuaded to withdraw its product. In its place the US government offered NSA "Clipper" chips for incorporation in secure phones. The chips would be manufactured by NSA, which would also record built-in keys and pass this information to other government agencies for storage and, if required, retrieval. This proposal proved extremely unpopular, and was abandoned. In its place, the US government proposed that <u>non</u> government agencies should be required to keep copies of every user's keys, a system called "key escrow" and, later, "key recovery". Viewed in retrospect, the actual purpose of these proposals was to provide NSA with a single (or very few) point(s) of access to keys, enabling them to continue to access private and commercial communications.

<u>Misrepresentation of law enforcement interception requirements</u>

84. Between 1993 to 1998, the United States conducted sustained diplomatic activity seeking to persuade EU nations and the OECD to adopt their "key recovery" system. Throughout this period, the US government insisted that the purpose of the initiative was to assist law enforcement agencies. Documents obtained for this study suggest that these claims wilfully misrepresented the true intention of US policy. Documents obtained under the US Freedom of Information Act indicate that policymaking was led exclusively by NSA officials, sometimes to the complete exclusion of police or judicial officials. For example, when the specially appointed US "Ambassador for Cryptography", David Aaron, visited Britain on 25 November 1996, he was accompanied and briefed by NSA's most senior representative in Britain, Dr James J Hearn, formerly Deputy Director of NSA. Mr Aaron had did not meet or consult FBI officials attached to his Embassy. His meeting with British Cabinet officials included NSA's representative and staff from Britain's GCHQ, but police officers or justice officials from both nations were excluded.

85. Since 1993, unknown to European parliamentary bodies and their electors, law enforcement officials from many EU countries and most of the UKUSA nations have been meeting annually in a separate forum to discuss their requirements for intercepting communications. These officials met under the auspices of a hitherto unknown organisation, ILETS (International Law Enforcement Telecommunications Seminar). ILETS was initiated and founded by the FBI. Table 2 lists ILETS meetings held between 1993 and 1997.

86. At their 1993 and 1994 meetings, ILETS participants specified law enforcement user requirements for communications interception. These appear in a 1974 ILETS document called "IUR 1.0". This document was based on an earlier FBI report on "Law Enforcement Requirements for the Surveillance of Electronic Communications", first issued in July 1992 and revised in June 1994. The IUR requirement differed little in substance from the FBI's requirements but was enlarged, containing ten requirements rather than nine. **IUR did not specify <u>any</u> law enforcement need for "key escrow" or "key recovery".** Cryptography was mentioned solely in the context of network security arrangements.

87. Between 1993 and 1997 police representatives from ILETS were not involved in the NSA-led policy making process for "key recovery", nor did ILETS advance any such proposal, even as late as 1997. Despite this, during the same period the US government repeatedly presented its policy as being motivated by the stated needs of law enforcement agencies. At their 1997 meeting in Dublin, ILETS did not alter the IUR. It was not until 1998 that a revised IUR was prepared containing requirements in respect of cryptography. It follows from this that the US government misled EU and OECD states about the true intention of its policy.

88. This US deception was, however, clear to the senior Commission official responsible for information security. In September 1996, David Herson, head of the EU Senior Officers' Group on Information Security, stated his assessment of the US "key recovery" project :

"'Law Enforcement' is a protective shield for all the other governmental activities … We're talking about foreign intelligence, that's what all this is about. There is no question [that] 'law enforcement' is a smoke screen".[56]

89. It should be noted that technically, legally and organisationally, law enforcement requirements for communications interception differ fundamentally from communications intelligence. Law enforcement agencies (LEAs) will normally witsh to intercept a specific line or group of lines, and must normally justify their requests to a judicial or administrative authority before proceeding. In contract, Comint agencies conduct broad international communications "trawling" activities, and operate under general warrants. Such operations do not require or even suppose that the parties they intercept are criminals. Such distinctions are vital to civil liberty, but risk being eroded it the boundaries between law enforcement and communications intelligence interception becomes blurred in future.

Year	*Venue*	*Non-EU participants*	*EU participants*
1993	Quantico, Virginia, USA	Australia, Canada, Hong Kong, Norway United States	Denmark, France, Germany, Netherlands, Spain, Sweden, United Kingdom
1994	Bonn, Germany	Australia, Canada, Hong Kong, Norway, United States	Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom
1995	Canberra, Australia	Australia, Canada, Hong Kong, New Zealand, Norway, United States	Belgium, France, Germany, Greece, Ireland, Italy, Netherlands, Spain, Sweden, United Kingdom
1997	Dublin, Ireland	Australia, Canada, Hong Kong, New Zealand, Norway, United States	Austria, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom

Table 2 ILETS meetings, 1993-1997

Law enforcement communications interception – policy development in Europe

90. Following the second ILETS meeting in Bonn in 1994, IUR 1.0 was presented to the Council of Ministers and was passed without a single word being altered on 17January 1995.[57] During 1995, several non EU members of the ILETS group wrote to the Council to endorse the (unpublished) Council resolution. The resolution was not published in the Official Journal for nearly two years, on 4 November 1996.

91. Following the third ILETS meeting in Canberra in 1995, the Australian government was asked to present the IUR to International Telecommunications Union (ITU). Noting that "law enforcement and national security agencies of a significant number of ITU member states have agreed on a generic set of requirements for legal interception", the Australian government asked the ITU to advise its standards bodies to incorporate the IUR requirements into future telecommunications systems on the basis that the "costs of [providing] legal interception capability and associated disruptions can be lessened by providing for that capability at the design stage".[58]

92. It appears that ILETS met again in 1998 and revised and extended its terms to cover the Internet and Satellite Personal Communications Systems such as Iridium. The new IUR also specified "additional security requirements for network operators and service providers", extensive new requirements for personal information about subscribers, and provisions to deal with cryptography.

93. On 3 September 1998, the revised IUR was presented to the Police Co-operation Working Group as ENFOPOL 98. The Austrian Presidency proposed that, as in 1994, the new IUR be adopted verbatim as a Council Resolution on interception "in respect of new technology".[59] The group did not agree. After repeated redrafting, a fresh paper has been prepared by the German Presidency, for the eventual consideration of Council Home and Justice ministers.[60]

5. Comint and economic intelligence

94. During the 1998 EP debate on "Transatlantic relations/ECHELON system" Commissioner Bangeman observed on behalf of the Commission that "If this system were to exist, it would be an intolerable attack against individual liberties, competition and the security of the states".[61] The existence of ECHELON was described in section 3, above. This section describes the organisational and reporting frameworks within which economically sensitive information collected by ECHELON and related systems is disseminated, summarising examples where European organisations have been the subject of surveillance.

Tasking economic intelligence

95. US officials acknowledge that NSA collects economic information, whether intentionally or otherwise. Former military intelligence attaché Colonel Dan Smith worked at the US Embassy, London until 1993. He regularly received Comint product from Menwith Hill. In 1998, he told the BBC that at Menwith Hill:

> *"In terms of scooping up communications, inevitably since their take is broadband, there will be conversations or communications which are intercepted which have nothing to do with the military, and probably within those there will be some information about commercial dealings"*
>
> *"Anything would be possible technically. Technically they can scoop all this information up, sort through it and find out what it is that might be asked for . . . But there is not policy to do this specifically in response to a particular company's interest*[62]

96. In general, this statement is not incorrect. But it overlooks fundamental distinctionS between tasking and dissemination, and between commercial and economic intelligence. There is no evidence that companies in any of the UKUSA countries are able to task Comint collection to suit their private purposes. They do not have to. Each UKUSA country authorises national level intelligence assessment organisations and relevant individual ministries to task and receive economic intelligence from Comint. Such information may be collected for myriad purposes, such as: estimation of future essential commodity prices; determining other nation's private positions in trade negotiations; monitoring international trading in arms; tracking sensitive technology; or evaluating the political stability and/or economic strength of a target country. Any of these targets and many others may produce intelligence of direct commercial relevance. The decision as to whether it should be disseminated or exploited is taken not by Comint agencies but by national government organisation(s).

Disseminating economic intelligence

97. In 1970, according to its former Executive Director, the US Foreign Intelligence Advisory Board recommended that "henceforth economic intelligence be considered a function of the national security, enjoying a priority equivalent to diplomatic, military, technological intelligence".[63] On 5 May 1977, a meeting between NSA, CIA and the Department of Commerce authorised the creation of secret new department, the "Office of Intelligence Liaison". Its task was to handle "foreign intelligence" of interest to the Department of Commerce. Its standing orders show that it was authorised to receive and handle SCI intelligence – Comint and Sigint from NSA. The creation of this office THUS provided a formal mechanism whereby NSA data could be used to support commercial and economic interests. After this system was highlighted in a British TV programme in 1993, its name was changed to the "Office of Executive Support".[64] Also in 1993, President Clinton extended US intelligence support to commercial organisations by creating a new National Economic Council, paralleling the National Security Council.

98. The nature of this intelligence support has been widely reported. "Former intelligence officials and other experts say tips based on spying … regularly flow from the Commerce Department to U.S. companies to help them win contracts overseas.[65] The Office of Executive Support provides classified weekly briefings to security officials. One US newspaper obtained reports from the Commerce Department demonstrating intelligence support to US companies:

> *One such document consists of minutes from an August 1994 Commerce Department meeting [intended] to identify major contracts open for bid in Indonesia in order to help U.S. companies win the work. A CIA employee … spoke at the meeting; five of the 16 people on the routine distribution list for the minutes were from the CIA.*

99. In the United Kingdom, GCHQ is specifically required by law (and as and when tasked by the British government) to intercept foreign communications "in the interests of the economic well-being of the United Kingdom ...in relation to the actions or intentions of persons outside the British Islands". Commercial interception is tasked and analysed by GCHQ's K Division. Commercial and economic targets can be specified by the government's Overseas Economic Intelligence Committee, the Economic Staff of the Joint Intelligence Committee, the Treasury, or the Bank of England.[66] According to a former senior JIC official, the Comint take routinely includes "company plans, telexes, faxes, and transcribed phone calls. Many were calls between Europe and the South[ern Hemisphere]".[67]

100. In Australia, commercially relevant Comint is passed by DSD to the Office of National Assesments, who consider whether, and if so where, to disseminate it. Staff there may pass information to Australian companies if they believe that an overseas nation has or seeks an unfair trade advantage. Targets of such activity have included Thomson-CSF, and trade negotiations with Japanese purchasers of coal and iron ore. Similar systems operate in the other UKUSA nations, Canada and New Zealand.

The use of Comint economic intelligence product

Panavia European Fighter Aircraft consortium and Saudi Arabia

101. In 1993, former National Security Council official Howard Teicher described in a programme about Menwith Hill how the European Panavia company was specifically targeted over sales to the Middle East. "I recall that the words 'Tornado' or 'Panavia' - information related to the specific aircraft - would have been priority targets that we would have wanted information about".[68]

Thomson CSF and Brazil

102. In 1994, NSA intercepted phone calls between Thomson-CSF and Brazil concerning SIVAM, a $1.3 billion surveillance system for the Amazon rain forest. The company was alleged to have bribed members of the Brazilian government selection panel. The contract was awarded to the US Raytheon Corporation - who announced afterwards that "the Department of Commerce worked very hard in support of U.S. industry on this project".[69] Raytheon also provide maintenance and engineering services to NSA's ECHELON satellite interception station at Sugar Grove.

Airbus Industrie and Saudi Arabia

103. According to a well-informed 1995 press report :"from a commercial communications satellite, NSA lifted all the faxes and phone calls between the European consortium Airbus, the Saudi national airline and the Saudi government. The agency found that Airbus agents were offering bribes to a Saudi official. It passed the information to U.S. officials pressing the bid of Boeing Co and McDonnell Douglas Corp., which triumphed last year in the $6 billion competition." [70]

International trade negotiations

104. Many other accounts have been published by reputable journalists and some firsthand witnesses citing frequent occasions on which the US government has utlitised Comint for national commercial purposes. These include targeting data about the emission standards of Japanese vehicles;[71] 1995 trade negotiations the import of Japanese luxury cars;[72] French participation in the GATT trade negotiations in 1993; the Asian-Pacific Economic Conference (APEC), 1997.

Targeting host nations

105. The issue of whether the United States utilises communications intelligence facilities such as Menwith Hilll or Bad Aibling to attack host nations' communications also arises. The available evidence suggests that such conduct may normally be avoided. According to former National Security Council official Howard Teicher, the US government would not direct NSA to spy on a host governments such as Britain:

> *"[But] I would never say never in this business because, at the end of the day, national interests are national interests … sometimes our interests diverge. So never say never - especially in this business".*

6. Comint capabilities after 2000

Developments in technology

106. Since the mid-1990s, communications intelligence agencies have faced substantial difficulties in maintaining global **access** to communications systems. These difficulties will increase during and after 2000. The major reason is the shift in telecommunications to high capacity optical fibre networks. Physical access to cables is required for interception. Unless a fibre network lies within or passes through a collaborating state, effective interception is practical only by tampering with optoelectronic repeaters (when installed). This limitation is likely to place many foreign land-based high capacity optical fibre networks beyond reach. The physical size of equipment needed to process traffic, together with power, communications and recording systems, makes clandestine activity impractical and risky.

107. Even where access is readily available (such as to COMSATs), the proliferation of new systems will limit **collection** activities, partly because budgetary constraint will restrict new deployments, and partly because some systems (for example, Iridium) cannot be accessed by presently available systems.

108. In the past 15 years the substantial technological lead in computers and information technology once enjoyed by Comint organisations has all but disappeared. Their principal computer systems are bought "off the shelf" and are the equal of or even inferior to those used by first rank industrial and academic organisations. They differ only in being "TEMPEST shielded", preventing them emitting radio signals which could be used to analyse Sigint activity.

109. Communications intelligence organisations recognise that the long war against civil and commercial cryptography has been lost. A thriving academic and industrial community is skilled in cryptography and cryptology. The Internet and the global marketplace have created a free flow in information, systems and software. NSA has failed in its mission to perpetuate access by pretending that that "key escrow" and like systems were intended to support law enforcement (as opposed to Comint) requirements.

110. Future trends in Comint are likely to include limits on investment in Comint collection from space; greater use of human agents to plant collection devices or obtain codes than in the past; and an intensified effort to attack foreign computer systems, using the Internet and other means (in particular, to gain access to protected files or communications before they are encrypted).

111. Attempts to restrict cryptography have nevertheless delayed the large-scale introduction of effective cryptographic security systems. The reduced cost of computational power has also enabled Comint agencies to deploy fast and sophisticated processing and sorting tools.

112. Recent remarks to CIA veterans by the head of staff of the US House of Representatives Permanent Select Committee on Intelligence, ex CIA officer John Millis illustrate how NSA views the same issues:

> *"Signals intelligence is in a crisis. … Over the last fifty years ... In the past, technology has been the friend of NSA, but in the last four or five years technology has moved from being the friend to being the enemy of Sigint.*
>
> *The media of telecommunications is no longer Sigint-friendly. It used to be. When you were doing RF signals, anybody within range of that RF signal could receive it just as clearly as the intended recipient. We moved from that to microwaves, and people figured out a great way to harness that as well. Well, we're moving to media that are very difficult to get to.*
>
> *Encryption is here and it's going to grow very rapidly. That is bad news for Sigint … It is going to take a huge amount of money invested in new technologies to get access and to be able to break out the information that we still need to get from Sigint".*

Policy issues for the European Parliament

1. The 1998 Parliamentary resolution on "Transatlantic relations/ECHELON system" [73] called for "protective measures concerning economic information and effective encryption". Providing such measures may be facilitated by developing an in-depth understanding of present and future Comint capabilities.

2. At the technical level, protective measures may best be focused on defeating hostile Comint activity by denying access or, where this is impractical or impossible, preventing processing of message content and associated traffic information by general use of cryptography.

3. As the SOGIS group within the Commission has recognised, [74] the contrasting interests of states is a complex issue. Larger states have made substantial investments in Comint capabilities. One member state is active in the UKUSA alliance, whilst others are either "third parties" to UKUSA or have made bilateral arrangements with NSA. Some of these arrangements were a legacy of the cold war; others are enduring. These issues create internal and international conflicts of interest. Technical solutions are not obvious. It should be possible to define a shared interest in implementing measures to defeat future external Comint activities directed against European states, their citizens and commercial activities.

4. A second area of apparent conflict concerns states' desires to provide communications interception for legitimate law enforcement purposes. The technical and legal processes involved in providing interception for law enforcement purpose differ fundamentally from those used in communications intelligence. Partly because of the lack of parliamentary and public awareness of Comint activities, this distinction is often glossed over, particularly by states that invest heavily in Comint. Any failure to distinguish between legitimate law enforcement interception requirements and interception for clandestine intelligence purposes raises grave issues for civil liberties. A clear boundary between law enforcement and "national security" interception activity is essential to the protection of human rights and fundamental freedoms.

5. At the present time, Internet browsers and other software used in almost every personal computer in Europe is deliberately disabled such that "secure" communications they send can, if collected, be read without difficulty by NSA. US manufacturers are compelled to make these arrangements under US export rules. A level playing field is important. Consideration could be given to a countermeasure whereby, if systems with disabled cryptographic systems are sold outside the United States, they should be required to conform to an "open standard" such that third parties and other nations may provide additional applications which restore the level of security to at least enjoyed by domestic US customers.

6. The work of ILETS has proceeded for 6 years without the involvement of parliaments, and in the absence of consultation with the industrial organisations whose vital interests their work affects. It is regrettable that, prior to the publication of this report, public information has not been available in states about the scope of the policy-making processes, inside and outside the EU, which have led to the formulation of existing and new law enforcement "user requirements". As a matter of urgency, the current policy-making process should be made open to public and parliamentary discussion in member states and in the EP, so that a proper balance may be struck between the security and privacy rights of citizens and commercial enterprises, the financial and technical interests of communications network operators and service providers, and the need to support law enforcement activities intended to suppress serious crime and terrorism.

Technical annexe

Broadband (high capacity multi-channel) communications

1. From 1950 until the early 1980s, high capacity multi-channel analogue communications systems were usually engineered using separate communications channels carried at different frequencies The combined signal, which could include 2,000 or more speech channels, was a "multiplex". The resulting "frequency division multiplex" (FDM) signal was then carried on a much higher frequency, such as by a microwave radio signal.

2. Digital communications have almost universally taken over from analogue methods. The basic system of digital multi-channel communications is time division multiplexing (TDM). In a TDM telephony system, the individual conversational channels are first digitised. Information concerning each channel is then transmitted sequentially rather than simultaneously, with each link occupying successive time "slots".

3. Standards for digital communications evolved separately within Europe and North America. In the United States, the then dominant public network carrier (the Bell system, run by AT&T) established digital data standards. The basic building block, a T-1 link, carries the equivalent of 24 telephone channels at a rate of 1.544 Mbps. Higher capacity systems operate at greater data transmission rates Thus, the highest transmission rate, T-5, carries the equivalent of 8,000 speech channels at a data rate of 560 Mbps.

4. Europe adopted a different framework for digital communications, based on standards originally agreed by the CEPT. The basic European standard digital link, E-1, carries 30 telephone channels at a data rate of 2 Mbps. Most European telecommunications systems are based on E-1 links or (as in North America), multiples thereof. The distinction is significant because most Comint processing equipment manufactured in the United States is designed to handle intercepted communications working to the European forms of digital communications.

5. Recent digital systems utilise synchronised signals carried by very high capacity optical fibres. Synchronising signals enables single channels to be easily extracted from high capacity links. The new system is known in the US as the synchronous optical network (SONET), although three equivalent definitions and labels are in use.[75]

Communications intelligence equipment

6. Dozens of US defence contractors, many located in Silicon Valley (California) or in the Maryland "Beltway" area near Washington, manufacture sophisticated Sigint equipment for NSA. Major US corporations, such as Lockheed Martin, Space Systems/Loral, TRW, Raytheon and Bendix are also contracted by NSA to operate major Sigint collection sites. A full report on their products and services is beyond the scope of this study. The state of the art in contemporary communications intelligence may usefully be demonstrated, however, by examining some of the Comint processing products of two specialist NSA niche suppliers: Applied Signal Technology Inc (AST), of Sunnyvale, California, and The IDEAS Operation of Columbia, Maryland (part of Science Applications International Corporation (SAIC)).[76]

7. Both companies include senior ex-NSA staff as directors. When not explicitly stated, their products can be identified as intended for Sigint by virtue of being "TEMPEST screened". AST states generally that its "equipment is used for signal reconnaissance of foreign telecommunications by the United States government". One leading cryptographer has aptly and and engagingly described AST as a "one-stop ECHELON shop".

Wideband extraction and signal analysis

8. Wideband (or broadband) signals are normally intercepted from satellites or tapped cables in the form of multiplex microwave or high frequency signals. The first step in processing such signals for Comint purposes is "**wideband extraction**". An extensive range of Sigint equipment is manufactured for this purpose, enabling newly intercepted systems to be surveyed and analysed. These include transponder survey equipment which identify and classify satellite downlinks, demodulators, decoders, demultiplexers, microwave radio link analysers, link survey units, carrier analysis systems, and many other forms of hardware and software.

9. A newly intercepted communications satellite or data link can be analysed using the AST Model 196 "Transponder characterisation system". Once its basic communications structure has been analysed, the Model 195 "Wideband snapshot analyser", also known as SNAPPER, can record sample data from even the highest capacity systems, sufficient to analyse communications in minute detail. By the start of 1999, operating in conjunction with the Model 990 "Flexible Data Acquisition Unit", this systems was able to record,

playback and analyse at data rates up to 2.488 Gbps (SONET OC-48). This is 16 times faster than the largest backbone links in general use on the Internet; larger than the telephony capacity of any current communications satellite; and equivalent to 40,000 simultaneous telephone calls. It can be fitted with 48 Gbyte of memory (500-1000 times larger than found in an average personal computer), enabling relatively lengthy recordings of high-speed data links. The 2.5 Gbps capacity of a single SNAPPER unit exceeds the current daily maximum data rate found on a typical large Internet exchange.[77]

10. Both AST and IDEAS offer a wide range of recorders, demultiplexers, scanners and processors, mostly designed to process European type (CEPT) E-1, E-3 (etc) signals at data rates of up to 160 Mbps. Signals may be recorded to banks of high-speed tape recorders, or into high capacity "RAID"[78] hard disk networks. Intercepted optical signals can be examined with the AST Model 257E "SONET analyser".

11. Once communications links have been analysed and broken down to their constituent parts, the next stage of Comint collection involves multi-channel processors which extract and filter messages and signals from the desired channels. There are three broad categories of interest: "voice grade channels", normally carrying telephony; fax communications; and analogue data modems. A wide selection of multi-channel Comint processors are available. Almost all of them separate voice, fax and data messages into distinct "streams" for downstream processing and analysis.

12. The AST Model 120 multi-channel processor – used by NSA in different configurations known as STARQUAKE, COBRA and COPPERHEAD - can handle 1,000 simultaneous voice channels and automatically extract fax, data and voice traffic. Model 128, larger still, can process 16 European E-3 channels (a data rate of 500 Mbps) and extract 480 channels of interest. The 1999 giant of AST's range, the Model 132 "Voice Channel Demultiplexer", can scan up to 56,700 communications channels, extracting more than 3,000 voice channels of interest. AST also provides Sigint equipment to intercept low capacity VSAT[79] satellite services used by smaller businesses and domestic users. These systems can be intercepted by the AST Model 285 SCPS processor, which identifies and extracts up to 48 channels of interest, distinguished between voice, fax and data.

13. According to US government publications, an early Wideband Extraction system was installed at NSA's Vint Hill Farms field station in 1970, about the time that systematic COMSAT interceptio collection began. That station is now closed. US publications identify the NSA/CSS Regional Sigint Operations Centre at San Antonio, Texas, as a site currently providing a multi-channel Wideband Extraction service.

Filtering, data processing, and facsimile analysis

14. Once communications channels have been identified and signals of interest extracted, they are analysed further by sophisticated workstations using special purpose software. AST's ELVIRA Signals Analysis Workstation is typical of this type of Sigint equipment. This system, which can be used on a laptop computer in covert locations, surveys incoming channels and extracts standard Comint data, including technical specifications (STRUM) and information about call destinations (SRI, or signal related information). Selected communications are relayed to distant locations using NSA standard "Collected Signals Data Format" (CSDF).[80]

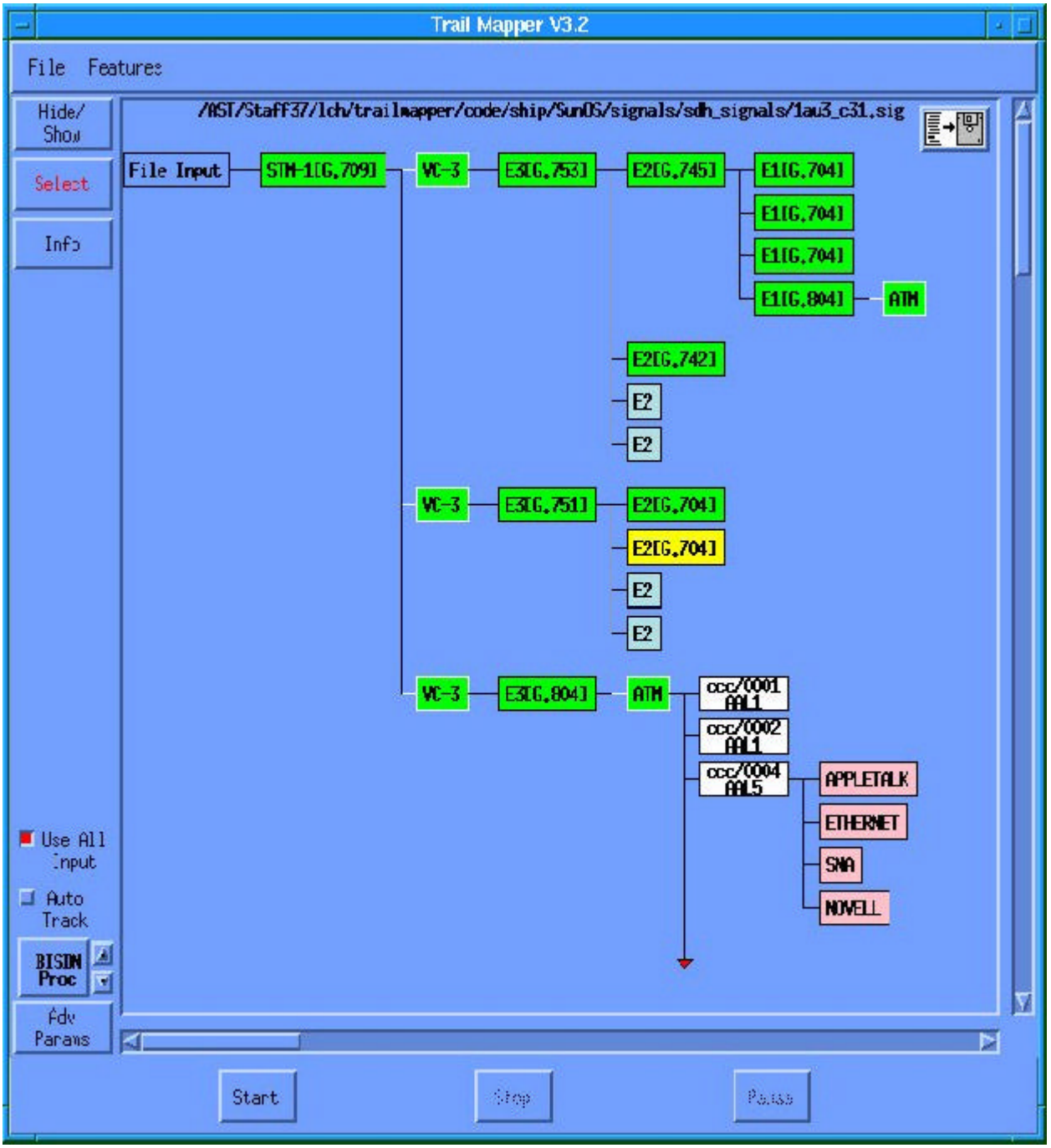
15. High-speed data systems can also be passed to AST's TRAILMAPPER software system, which works at a data rate of up to 2.5 Gbps. It can interpret and analyse every type of telecommunications system, including European, American and optical standards. TRAILMAPPER appears to have been designed with a view to analysing ATM (asynchronous transfer mode) communications. ATM is a modern, high-capacity digital communications system. It is better suited than standard Internet connections to carrying multimedia traffic and to providing business with private networks (VPN, LAN or WAN). TRAILMAPPER will identify and characterise such business networks.

16. In the next stage downstream, intercepted signals are processed according to whether they are voice, fax or data. AST's "Data Workstation" is designed to categorise all aspects of data communications, including systems for handling e-mail or sending files on the Internet.[81] Although the very latest modem systems (other than ISDN) are not included in its advertised specification, it is clear from published research that AST has developed the technology to intercept and process the latest data communications systems used by individuals and business to access the Internet.[82] The Data Workstation can stored and automatically process 10,000 different recorded signals.

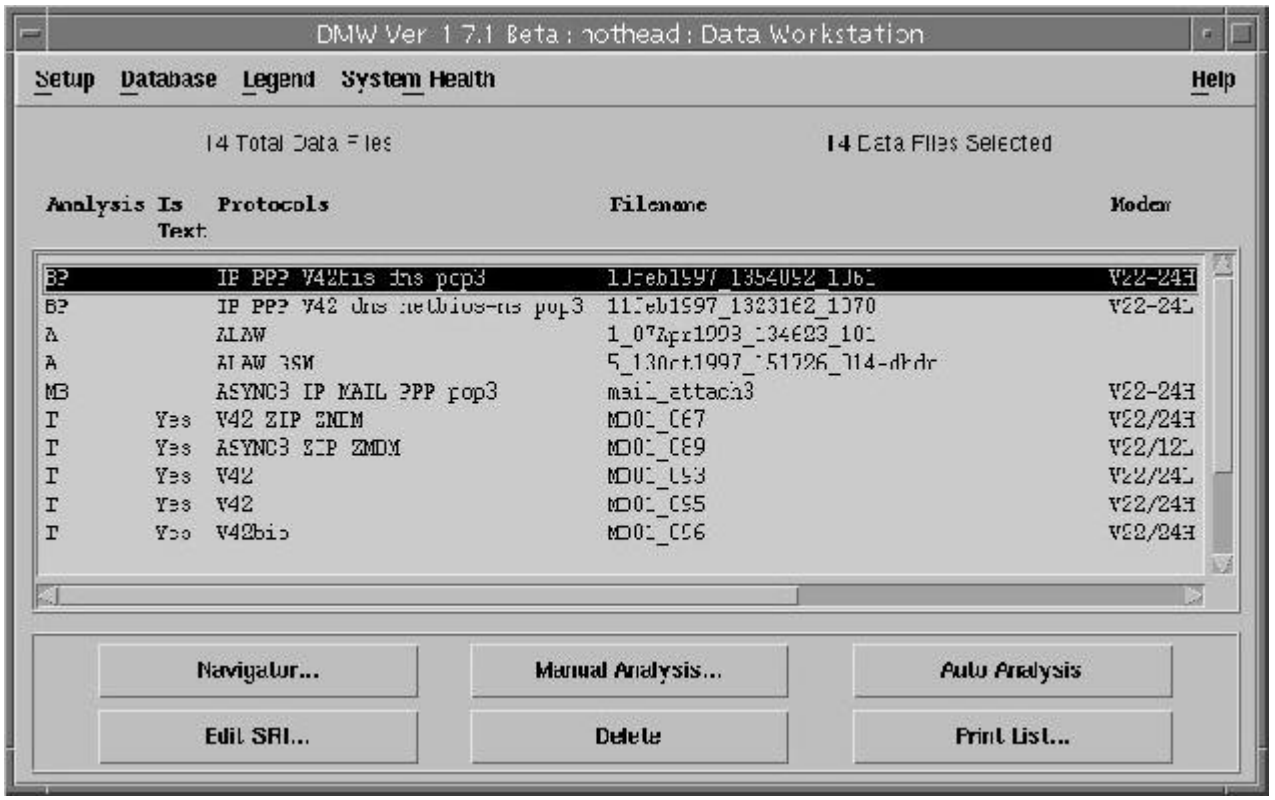
17. Fax messages are processed by AST's Fax Image Workstation. This is described as a "user friendly, interactive analysis tool for rapid examination images stored on disk. Although not mentioned in AST's literature, standard fax pre-processing for Dictionary computers involves automatic "optical character

recognition" (OCR) software. This turns the typescript into computer readable (and processable) text. The effectiveness of these systems makes fax-derived Comint an important collection subsystem. It has one drawback. OCR computer systems that can reliably recognise handwriting do not exist. No one knows how to design such a system. It follows that, perversely, hand-written fax messages may be a secure form of communication that can evade Dictionary surveillance criteria, provided always that the associated "signal related information" (calling and receiving fax numbers) have not been recognised as being of interest and directed to a Fax Image Workstation.

18. AST also make a "Pager Identification and Message Extraction" system which automatically collects and processes data from commercial paging systems. IDEAS offer a Video Teleconferencing Processor that can simultaneously view or record two simultaneous teleconferencing sessions. Sigint systems to intercept cellular mobile phone networks such as GSM are not advertised by AST or IDEAS, but are available from other US contractors. The specifications and ready availability of such systems indicate how industrialised and pervasive Comint has became. It has moved far from the era when (albeit erroneously), it was publicly associated only with monitoring diplomatic or military messages.



NSA "Trailmapper" software showing automatic detection of private networks inside intercepted high capacity STM-1 carrier



The "Data Workstation" software system analyses up to 10,000 recorded messages, identifying Internet traffic, e-mail messages and attachments

Traffic analysis, keyword recognition, text retrieval, and topic analysis

19. Traffic analysis is a method of obtaining intelligence from signal related information, such as the number dialled on a telephone call, or the Calling Line Identification Data (CLID) which identifies the person making the call. Traffic analysis can be used where message content is not available, for example when encryption is used. By analysing calling patterns, networks of personal associations may be analysed and studied. This is a principal method of examining voice communications.

20. Whenever machine readable communications are available, keyword recognition is fundamental to Dictionary computers, and to the ECHELON system. The Dictionary function is straightforward. Its basic mode of operation is akin to web search engines. The differences are of substance and of scale. Dictionaries implement the tasking of their host station against the entire mass of collected communications, and automate the distribution of selected raw product.

21. Advanced systems have been developed to perform very high speed sorting of large volumes of intercepted information. In the late 1980s, the manufacturers of the RHYOLITE Sigint satellites, TRW, designed and manufactured a Fast Data Finder (FDF) microchip for NSA. The FDF chip was declassified in 1972 and made available for commercial use by a spin-off company, Paracel. Since then Paracel has sold over 150 information filtering systems, many of them to the US government. Paracel describes its current FDF technology as the "fastest, most accurate adaptive filtering system in the world":

> *A single TextFinder application may involve trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles … the TextFinder chip implements the most comprehensive character-string comparison functions of any text retrieval system in the world.*

Devices like this are ideal for use in ECHELON and the Dictionary system.

22. A lower capacity system, the PRP-9800 Pattern Recognition Processor, is manufactured by IDEAS. This is a computer card which can be fitted to a standard PC. It can analyse data streams at up to 34 Mbps (the European E-3 standard), matching every single bit to more than 1000 pre-selected patterns.

23. Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may soon seem archaic. **Topic analysis** is a more powerful and intuitive technique, and one that NSA is developing and promoting with confidence. Topic analysis enables Comint customers to ask their computers to "find me documents about subject X". X might be "Shakespeare in love" or "Arms to Iran".

24. In a standard US test used to evaluate topic analysis systems,[83] one task the analysis program is given is to find information about "Airbus subsidies". The traditional approach involves supplying the computer with the key terms, other relevant data, and synonyms. In this example, the designations A-300 or A-320 might be synonymous with "Airbus". The disadvantage of this approach is that it may find irrelevant intelligence (for example, reports about export subsidies to goods flown on an Airbus) and miss relevant material (for example a financial analysis of a company in the consortium which does not mention the Airbus product by name). Topic analysis overcomes this and is better matched to human intelligence.

25. The main detectable thrust of NSA research on topic analysis centres on a method called N-gram analysis. Developed inside NSA's Research group - responsible for Sigint automation - N-gram analysis is a fast, general method of sorting and retrieving machine-readable text according to language and/or topic. The N-gram system is claimed to work independently of the language used or the topic studied. NSA patented the method in 1995.[84]

26. To use N-gram analysis, the operator ignores keywords and defines the enquiry by providing the system with selected written documents concerning the topic of interest. The system determines what the topic is from the seed group of documents, and then calculates the probability that other documents cover the same topic. In 1994, NSA made its N-gram system available for commercial exploitation. NSA's research group claimed that it could be used on "very large data sets (millions of documents)", could be quickly implemented on any computer system and that it could operate effectively "in text containing a great many errors (typically 10-15% of all characters)".

27. According to former NSA Director William Studeman, "information management will be the single most important problem for the (US) Intelligence Community" in the future.[85] Explaining this point in 1992, he described the type of filtering involved in systems like ECHELON:

> *One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report Is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.*

Speech recognition systems

28. For more than 40 years, NSA, ARPA, GCHQ and the British government Joint Speech Research Unit have conducted and sponsored research into speech recognition. Many press reports (and the previous STOA report) have suggested that such research has provided systems which can automatically select telephone communications of intelligence interest based on the use of particular "key words" by a speaker. If available, such systems would enable vastly more extensive Comint information to be gathered from telephone conversations than is available from other methods of analysis. The contention that telephone word-spotting systems are readily available appears to by supported by the recent availability of a string of low-cost software products resulting from this research. These products permit PC users to dictate to their computers instead of entering data through the keyboard. [86]

29. The problem is that for Comint applications, unlike personal computer dictation products, speech recognition systems have to operate in a multi-speaker, multi-language environment where numerous previously never heard speakers may each feature physiological differences, dialect variations, and speech traits. Commercial PC systems usually require one or more hours of training in order reliably to recognise a single speaker. Even then, such systems may mistranscribe 10% or more of the words spoken.

30. In PC dictation applications, the speaker can correct mistranscriptions and continually retrain the recognition system, making a moderate error rate acceptable. For use in Comint, where the interception system has no prior knowledge of what has been said (or even the language in use), and has to operate in the poorer signal environment of a telephone speech channel, such error rates are unachievable. Worse still, even moderate error rates can make a keyword recognition system worthless by generating both false positive outputs (words wrongly identified as keywords) and false negative outputs (missing genuine keywords).

31. This study has found no evidence that voice keyword recognition systems are currently operationally deployed, nor that they are yet sufficiently accurate to be worth using for intelligence purposes.

Continuous speech recognition

32. The fundamental technique in many speech recognition applications is a statistical method called Hidden Markov Modelling (HMM). HMM systems have been developed at many centres and are claimed academically to offer "good word spotting performance … using very little or no acoustic speech training".[87] The team which reported this result tested its system using data from the US Department of Defense "Switchboard Data", containing recordings of thousand of different US telephone conversations. On a limited test the probabilities of correctly detecting the occurrences of 22 keywords ranged from 45-68% on settings which allowed for 10 false positive results per keyword per hour. Thus if 1000 genuine keywords appeared during an hour's conversation, there would be at least 300 missed key words, plus 220 false alarms.

33. At about the same time, (February 1990), the Canadian Sigint organisation CSE awarded a Montreal-based computer research consultancy the first of a series of contracts to develop a Comint wordspotting system.[88] The goal of the project was to build a word-spotter that worked well even for noisy calls. Three years later, CRIM reported that "our experience has taught us that, regardless of the environmental conditions, wordspotting remains a difficult problem". The key problem, which is familiar to human listeners, is that a single word heard on its own can easily be misinterpreted, whereas in continuous speech the meaning may be deduced from surrounding words. CRIM concluded in 1993 that "it is probable that the most effective way of building a reliable wordspotter is to build a large vocabulary continuous speech recognition (CSR) system".

34. Continuous speech recognition software working in real time needs a powerful fast, processor. Because of the lack of training and the complex signal environment found in intercepted telephone calls, it is likely that even faster processors and better software than used in modern PCs would yield poorer results than are now provided by well-trained commercial systems. Significantly, an underlying problem is that voice keyword recognition is, as with machine-readable messages, an imperfect means to the more useful intelligence goal - **topic spotting**.

35. In 1993, having failed to build a workable wordspotter, CRIM suggesting "bypassing" the problem and attempting instead to develop a voice topic spotter. CRIM reported that "preliminary experiments reported at a recent meeting of American defense contractors … indicate that this may in fact be an excellent approach to the problem". They offered to produce an "operational topic spotting" system by 1995. They did not succeed. Four years later, they were still experimenting on how to built a voice topic spotter.[89] They received a further research contract. One method CRIM proposed was NSA's N-gram technique.

Speaker identification and other voice message selection techniques

36. In 1993, CRIM also undertook to supply CSE with an operational speaker identification module by March 1995. Nothing more was said about this project, suggesting that the target may have been met. In the same year, according to NSA documents, the IDEAS company supplied a "Voice Activity Detector and Analyser", Model TE464375-1, to NSA's offices inside GCHQ Cheltenham. The unit formed the centre of a 14-position computer driven voice monitoring system. This too may have been an early speaker identification system.

37. In 1995, widely quoted reports suggested that NSA speaker identification had been used to help capture the drug cartel leader Pablo Escobar. The reports bore strong resemblance to a novel by Tom Clancy, suggesting that the story may have owed more to Hollywood than high tech. In 1997, the Canadian CRE awarded a contract to another researcher to develop "new retrieval algorithms for speech characteristics used for speaker identification", suggesting this method was not by then a fully mature technology. According to Sigint staff familiar with the current use of Dictionary, it can be programmed to search to identify particular speakers on telephone channels. But speaker identification is still not a particularly reliablr or effective Comint technique.[90]

38. In the absence of effective wordspotting or speaker identification techniques, NSA has sought alternative means of automatically analysing telephone communications. According NSA's classification guide, other techniques examined include Speech detection – detecting the presence or absence of speech activity; Speaker discrimination – techniques to distinguish between the speech of two or more speakers; and Readability estimation – techniques to determine the quality of speech signals. System descriptions must be classified "secret" if NSA "determines that they represent major advances over techniques known in the research community".[91]

"Workfactor reduction"; the subversion of cryptographic systems

39. From the 1940s to date, NSA has undermined the effectiveness of cryptographic systems made or used in Europe. The most important target of NSA activity was a prominent Swiss manufacturing company, Crypto AG. Crypto AG established a strong position as a supplier of code and cypher systems after the second world war. Many governments would not trust products offered for sale by major powers. In contrast, Swiss companies in this sector benefited from Switzerland's neutrality and image of integrity.

40. NSA arranged to rig encryption systems sold by Crypto AG, enabling UKUSA agencies to read the coded diplomatic and military traffic of more than 130 countries. NSA's covert intervention was arranged through the company's owner and founder Boris Hagelin, and involved periodic visits to Switzerland by US "consultants" working for NSA. One was Nora L MacKabee, a career NSA employee. A US newspaper obtained copies of confidential Crypto AG documents recording Ms Mackebee's attendance at discussion meetings in 1975 to design a new Crypto AG machine".[92]

41. The purpose of NSA's interventions were to ensure that while its coding systems should appear secure to other cryptologists, it was not secure. Each time a machine was used, its users would select a long numerical key, changed periodically. Naturally users wished to selected their own keys, unknown to NSA. If Crypto AG's machines were to appear strong to outside testers, then its coding system should work, and actually be strong. NSA's solution to this apparent condundrum was to design the machine so that it broadcast the key it was using to listeners. To prevent other listeners recognising what was happening, the key too had also to be sent in code - a different code, known only to NSA. Thus, every time NSA or GCHQ intercepted a message sent using these machines, they would first read their own coded part of the message, called the "*hilfsinformationen*" (help information field) and extract the key the target was using. They could then read the message itself as fast or even faster than the intended recipient[93]

42. The same technique was re-used in 1995, when NSA became concerned about cryptographic security systems being built into Internet and E-mail software by Microsoft, Netscape and Lotus. The companies agreed to adapt their software to reduce the level of security provided to users outside the United States. In the case of Lotus Notes, which includes a secure e-mail system, the built-in cryptographic system uses a 64 bit encryption key. This provides a medium level of security, which might at present only be broken by NSA in months or years.

43. Lotus built in an NSA "help information" trapdoor to its Notes system, as the Swedish government discovered to its embarrassment in 1997. By then, the system was in daily use for confidential mail by Swedish MPs, 15,000 tax agency staff and 400,000 to 500,000 citizens. Lotus Notes incorporates a "workfactor reduction field" (WRF) into all e-mails sent by non US users of the system. Like its predecessor the Crypto AG "help information field" this device reduces NSA's difficulty in reading European and other e-mail from an almost intractable problem to a few seconds work. The WRF broadcasts 24 of the 64 bits of the key used for each communication. The WRF is encoded, using a "public key" system which can only be read by NSA. Lotus, a subsidiary of IBM, admits this. The company told *Svenska Dagbladet*:

> *"The difference between the American Notes version and the export version lies in degrees of encryption. We deliver 64 bit keys to all customers, but 24 bits of those in the version that we deliver outside of the United States are deposited with the American government".*[94]

44. Similar arrangements are built into all export versions of the web "browsers" manufactured by Microsoft and Netscape. Each uses a standard 128 bit key. In the export version, this key is not reduced in length. Instead, 88 bits of the key are broadcast with each message; 40 bits remain secret. It follows that almost every computer in Europe has, as a built-in standard feature, an NSA workfactor reduction system to enable NSA (alone) to break the user's code and read secure messages.

45. The use of powerful and effective encryption systems will increasingly restrict the ability of Comint agencies to **process** collected intelligence. "Moore's law" asserts that the cost of computational power halves every 18 months. This affects both the agencies and their targets. Cheap PCs can now efficiently perform complex mathematical calculations need for effective cryptography. In the absence of new discoveries in physics or mathematics Moore's law favours codemakers, not codebreakers.

Glossary and definitions

ATM	Asynchronous Transfer Mode; a high speed form of digital communications increasingly used for on the Internet
BND	Bundesachrichtendienst; the foreign intelligence agency of the Federal Republic of Germany. Its functions include Sigint
CCITT	Consultative Committee for International Telephony and Telegraphy; United Nations agency developing standards and protocols for telecommunications; part of the ITU; also known as ITU-T
CEPT	Conference Europeene des Postes et des Telecommunications
CLID	Calling Line Identification Data
Comint	Communications Intelligence
COMSAT	(Civil/commercial) communications satellite; for military communications usage, the phraseology is commonly reversed, i.e., SATCOM.
CRIM	Centre de Recherche Informatique de Montreal
CSDF	Collected Signals Data Format; a term used only in Sigint
CSE	Communications Security Establishment, the Sigint agency of Canada
CSS	Central Security Service; the military component of NSA
DARPA	Defense Advanced Research Projects Agency (United States Department of Defense)
DGSE	Directorate General de Securite Exteriere, the foreign intelligence agency of France. Its functions include Sigint
DSD	Defence Signals Directorate, the Sigint agency of the Commonwealth of Australia
DODJOCC	Department of Defense Joint Operations Centre Chicksands
E1, E3 (etc)	Standard for digital or TDM communications systems defined by the CEPT, and primarily used within Europe and outside North America
ENFOPOL	EU designation for documents concerned with law enforcement matters/police
FAPSI	Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii, the Federal Agency for Government Communications and Information of Russia. Its functions include Sigint
FBI	Federal Bureau of Investigation; the national law enforcement and counter-intelligence agency of the United States
FDF	Fast Data Finder
FDM	Frequency Division Multiplex; a form of multi-channel communications based on analogue signals
FISA	Foreign Intelligence Surveillance Act (United States)
FISINT	Foreign Instrumentation Signals Intelligence, the third branch of Sigint
Gbps	Gigabits per second
GCHQ	Government Communications Headquarters; the Sigint agency of the United Kingdom
GHz	GigaHertz
Gisting	Within Sigint, the analytical task of replacing a verbatim text with the sense or main points of a communication
HDLC	High-level Data Link Control
HF	High Frequency; frequencies from 3MHz to 30MHz
HMM	Hidden Markov Modelling, a technique widely used in speech recognition systems.
ILETS	International Law Enforcement Telecommunications Seminar
Intelsat	International Telecommunications Satellite
IOSA	Interim Overhead Sigint Architecture
Iridium	Satellite Personal Communications System involving 66 satellites in low earth orbit, providing global communications from mobile telephones
ISDN	Integrated Services Data Network
ISP	Internet Service Provider
ITU	International Telecommunications Union
IUR	International User Requirements (for communications interception); IUR 1.0 was prepared by ILETS (*qv*) in 1994
IXP	Internet Exchange Point
LAN	Local Area Network
LEA	Law Enforcement Agency (American usage)

Mbps	Megabits per second
MHz	MegaHertz
Microwave	Radio signals with wavelengths of 10cm or shorter; frequencies above 1GHz
Modem	Device for sending data to and from (e.g.) a computer; a “modulator-demodulator)
MIME	Multipurpose Internet Message Extension; a systems used for sending computer files, images, documents and programs as "attachments" to an e-mail message
N-gram analysis	A system for analysing textual documents; in this context, a system for matching a large group of documents to a smaller group embodying a topic of interest. The method depends on counting the frequency with which character groups of length N appear in each document; hence N-gram
NSA	National Security Agency, the Sigint agency of the United States
OCR	Optical Character Recognition
PC	Personal Computer
PCS	Personal Communications Systems; the term includes mobile telephone systems, paging systems and future wide area radio data links for personal computers, etc
POP (or POP3)	Post Office Program; a system used for receiving and holding e-mail
PTT	Posts Telegraph and Telephone (Administration or Authority)
RAID	Redundant Array of Inexpensive Disks
SCI	Sensitive Compartmented Intelligence; used to limit access to Comint information according to "compartments"
SCPC	Single Channel Per Carrier; low capacity satellite communications system
SMTP	Standard Mail Transport Protocol
Sigint	Signals Intelligence
SONET	Synchronous Optical Network
SMDS	Switched Multi-Megabit Data Service
SMO	Support for Military Operations
SPCS	Satellite Personal Communications Systems
SRI	Signal Related Information; a term used only in Sigint
STOA	Science and Technology Assessments Office of the European Parliament; the body commissioning this report
T1, T3 (etc)	Digital or TDM communications systems originally defined by the Bell telephone system in North America, and primarily used there
TCP/IP	Terminal Control Protocol/Internet Protocol
TDM	Time Division Muliplex; a form of multi-channel communications normally based on digital signals
Traffic analysis	Within Sigint, a method of analysing and obtaining intelligence from messages without reference to their content; for example by studying the origin and destination of messages with a view to eliciting the relationship between sender and recipient, or groups thereof
UKUSA	UK-USA agreement
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal; low capacity satellite communications system serving home and business users
WAN	Wide Area Network
WRF	Workfactor Reduction Field
WWW	World Wide Web

X.25, V.21, V.34, V.90, V.100 (etc) are CCITT telecommunications standards

Illustrations : page 5; US Air Force; IPTV Ltd; page 6; Stephen King, Charles V Pick; IPTV Ltd; page 8; Jim Bamford, GCHQ; page 9; US Navy, KGB/Russian Security Service; page 12; D Campbell.

Notes

[1.] UKUSA refers to the 1947 United Kingdom – United States agreement on Signals intelligence. The nations of the UKUSA alliance are the United States (the "First Party"), United Kingdom, Canada, Australia and New Zealand (the "Second Parties").
[2.] "An appraisal of the Technologies of Political Control", Steve Wright, Omega Foundation, European Parliament (STOA), 6 January 1998.
[3.] "They've got it taped", Duncan Campbell, *New Statesman*, 12 August 1988. "Secret Power : New Zealand's Role in the International Spy Network", Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, 1996.
4. National Security Council Intelligence Directive No 6, National Security Council of the United States, 17 February 1972 (first issued in 1952).
[5.] SIGINT is currently defined as consisting of COMINT, ELINT (electronic or non-communications intelligence and FISINT (Foreign Instrumentation Signals Intelligence).
[6.] Statement by Martin Brady, Director of DSD, 16 March 1999. Broadcast on the *Sunday Programme*, Channel 9 TV (Australia), 11 April 1999.
[7.] "Farewell", despatch to all NSA staff, William Studeman, 8 April 1992. The two business areas to which Studeman referred were "increased global access" and "SMO" (support to military operations).
[8.] *Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii*, the (Russian) Federal Agency for Government Communications and Information. FAPSI's functions extend beyond Comint and include providing government and commercial communications systems.
9. Private communications from former NSA and GCHQ employees.
[10.] Sensitive Compartmented Intelligence.
11. See note 1.
[12.] Private communications from former GCHQ employees; the US Act is the Foreign Intelligence Surveillance Act (FISA).
13. See note 6.
[14.] In 1919, US commercial cable companies attempted to resist British government demands for access to all cables sent overseas. Three cable companies testified to the US Senate about these practices in December 1920. In the same year, the British Government introduced legislation (the Official Secrets Act, 1920, section 4) providing access to all or any specified class of communications. The same power was recodified in 1985, providing lawful access for Comint purposes to all "external communications", defines as any communications which are sent from or received outside the UK (Interception of Communication Act 1984, Section 3(2)). Similar requirements on telecommunications operators are made in the laws of the other UKUSA countries. See also "Operation SHAMROCK", (section 3).
[15.] "The Puzzle Palace", James Bamford, Houghton Mifflin, Boston, 1982, p331.
[16.] Personal communications from former NSA and GCHQ employees.
[17.] "Dispatches : The Hill", transmitted by Channel 4 Television (UK), 6 October 1993. DODJOCC stood for Department of Defense Joint Operations Centre Chicksands.
[18.] "The Justice Game", Geoffrey Robertson, Chapter 5, Chatto and Windus, London, 1998
[19.] Fink report to the House Committee on Government Operations, 1975, quoted in "NSA spies on the British government", *New Statesman,* 25 July 1980
20. "Amerikanskiye sputniki radioelektronnoy razvedki na Geosynchronnykh orbitakh" ("American Geosynchronous SIGINT Satellites"), Major A Andronov, *Zarubezhnoye Voyennoye Obozreniye,* No.12, 1993, pps 37-43.
[21.] "Space collection", in The US Intelligence Community (fourth edition), Jeffrey Richelson, Westview, Boulder, Colorado, 1999, pages 185-191.
[22.] See note 18.
23. Richelson, *op cit.*
[24.] "UK Eyes Alpha", Mark Urban, Faber and Faber, London, 1996, pps 56-65.
[25.] Besides the stations mentioned, a major ground station whose targets formerly included Soviet COMSATs is at Misawa, Japan. Smaller ground stations are located at Cheltenham, England; Shoal Bay, Australia.
[26.] "Sword and Shield : The Soviet Intelligence and Security Apparatus", Jeffrey Richelson, Ballinger, Cambridge, Massachusetts, 1986.
[27.] "Les Francais aussi ecountent leurs allies", Jean Guisnel, *Le Point*, 6 June 1998.
[28.] *Intelligence* (Paris), **93**, 15 February 1999, p3.

[29.] "Blind mans Bluff : the untold story of American submarine espionage", Sherry Sontag and Christopher Drew, Public Affairs, New York, 1998.
30. *Ibid.*
[31.] *Ibid*
[32.] A specimen of the IVY BELLS tapping equipment is held in the former KGB museum in Moscow. It was used on a cable running from Moscow to a nearby scientific and technical institution.
[33.] TCP/IP. TCP/IP stands for Terminal Control Protocol/Internet Protocol. IP is the basic network layer of the Internet.
[34.] GCHQ website at http://www.gchq.gov.uk/technol.html
[35.] Personal communication from DERA. A Terabyte is one thousand Gigabytes, i.e., 1012 bytes.
36. Personal communication from John Young.
37. "Puzzle palace conducting internet surveillance", Wayne Madsen, Computer Fraud and Security Bulletin, June 1995.
38. *Ibid.*
[39.] "More Naked Gun than Top Gun", Duncan Campbell, *Guardian,* 26 November 1997.
[40.] "Spyworld", Mike Frost and Michel Gratton, Doubleday Canada, Toronto, 1994.
[41.] The National Security Agency and Fourth Amendment Rights, Hearings before the Select Committee to Study Government Operations with Respect to Intelligence Activitities, US Senate, Washington, 1976.
42. Letter from, Lt Gen Lew Allen, Director of NSA to US Attorney General Elliot Richardson, 4 October 1973; contained in the previous document.
[43.] Private communication.
[44.] World in Action, Granada TV.
[45.] This arrangements appears to be an attempt to comply with legal restrictions in the Interception of Communications Act 1985, which prohibit GCHQ from handling messages except those identified in government "certificates" which "describe the intercepted material which should be examined". The Act specifies that "so much of the intercepted material as is not certified by the certificate is not [to be] read, looked at or listened to by any person". It appears from this that, although all messages passing through the United Kingdom are intercepted and sent to GCHQ's London office, the organisation considers that by having British Telecom staff operate the Dictionary computer, it is still under the control of the telecommunications network operator unless and until it is selected by the Dictionary and passes from BT to GCHQ.
[46.] Private communications.
[47.] "Naval Security Group Detachment, Sugar Grove History for 1990", US Navy, 1 April 1991.
[48.] Missions, functions and tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia", NAVSECGRU INSTRUCTION C5450.48A, 3 September 1991.
[49.] Report on tasks of Detachment 3 , 544 Air Intelligence Group, *Air Intelligence Agency Almanac*, US Air Force, 1998-99.
[50.] *Ibid,* Detachment 2, 544 Air Intelligence Group.
[51.] Information obtained by Bill Robinson, Conrad Grebel College, Waterloo, Ontario. CDF and CFS documents were obtained under the Freedom of Information Act, or published on the World Wide Web.
[52.] Career resume of Patrick D Duguay, published at: http://home.istar.ca/~pdduguay/resume.htm.
[53.] CSE Financial Status Report, 1 March 1996, released under the Freedom of Information Act. Further details about "ECHELON" were not provided. It is therefore ambiguous as to whether the expenditure was intended for the ECHELON computer system, or for different functions (for example telecommunications or power services).
[54.] "Secret Power", *op cit.*
[55.] *Twenty/Twenty*, TV3 (New Zealand), October 1999.
[56.] Interview with David Herson, Head of Senior Officers' Group on Information Security, EU, by staff of *Engineering Weekly* (Denmark), 25 September 1996. Published at http://www.ing.dk/arkiv/herson.htm
[57.] Council Resolution on the Lawful Interception of Telecommunications, 17 January 1995, (96C_329/01)
[58.] "International Harmonisation of Technical Requirements for Legal Interception of Telecommunications", Resolution 1115, Tenth Plenary meeting of the ITU Council, Geneva, 27 June 1997.
[59.] ENFOPOL 98, Draft Resolution of the Council on Telecommunications Interception in respect of New Technology. Submitted by the Austrian Presidency. Brussels, 3 September 1998.
[60.] ENFOPOL 19, 13 March 1999.
[61.] European Parliament, 14 September 1998.
[62.] "Uncle Sam's Eavesdroppers", Close Up North, BBC North, 3 December 1998; reported in "Star Wars strikes back", *Guardian*, 3 December 1998
[63.] "Dispatches : The Hill", Channel 4 Television (UK), 6 October 1993
[64.] *Ibid.*
[65.] "Mixing business with spying; secret information is passed routinely to U.S.", Scott Shane, *Baltimore Sun*, 1 November 1996.
[66.] "UK Eyes Alpha", *op cit,* p235.
[67.] Private communication.
[68.] See note 62.

[69.] Raytheon Corp press release: published at: http://www.raytheon.com/sivam/contract.html
70. "America's Fortress of Spies", Scott Shane and Tom Bowman, Baltimore Sun 3 December 1995.
[71.] "Company Spies", Robert Dreyfuss, *Mother Jones*, May/June 1994.
[72.] *Financial Post*, Canada, 28 February 1998.
[73.] European Parliament, 16 September 1998.
[74.] See note 56.
[75.] Equivalent communications may be known as Synchronous Transport Module (STM) signals within the Synchronous Digital Hierarchy (ITU standard); Synchronous Transport Signals (STS) within the US SONET system; or as Optical Carrier signals (OC).
[76.] The information about these Sigint systems has been drawn from open sources (only).
[77.] In April 199, the peak data rate at MAE West was less than 1.9 Gbps.
[78.] Redundant Arrays of Inexpensive Disks.
[79.] Very Small Aperture Terminal; SCPC is Single Channel Per Carrier.
[80.] "Collected Signals Data Format"; defined in US Signals Intelligence Directive 126 and in NSA's CSDF manual. Two associated NSA publications providing further guidance are the Voice Processing Systems Data Element Dictionary and the Facsimile Data Element Dictionary, both issued in March 1997.
[81.] The Data Workstation processes TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100, and modem protocols up to and including V.42 (see glossary).
[82.] "Practical Blind Demodulators for high-order QAM signals", J R Treichler, M G Larimore and J C Harp, *Proc IEEE,* **86**, 10, 1998, p1907. Mr Treichler is technical director of AST. The paper describes a system used to intercept multiple V.34 signals, extendable to the more recent protocols.
[83.] The tasks were set in the second Text Retrieval conference(TREC) organised by the ARPA and the US National Institute of Science and Technology (NIST), Gaithersburg, Maryland. The 7th annual TREC conference took place in Maryland in 1999.
[84.] "Method of retrieving documents that concern the same topic"; US Patent number 5418951, issued 23 May 1995; inventor, Marc Damashek; rights assigned to NSA.
[85.] Address to the Symposium on "National Security and National Competitiveness : Open Source Solutions" by Vice Admiral William Studeman, Deputy Director of Central Intelligence and former director of NSA, 1 December 1992, McLean, Virginia.
86. For example, IBM *Via Voice*, Dragon *Naturally Speaking,* Lemout and Hauspe *Voice Xpress.*
[87.] "A Hidden Markov Model based keyword recognition system", R.C.Rose and D.B.Paul, *Proceedings of the International Conference on Accoustics, Speech and Signal processing*, April 1990.
[88.] Centre de Recherche Informatique de Montreal.
[89.] "Projet detection des Themes", CRIM, 1997; published at http://www.crim.ca/adi/projet2.html.
[90.] Private communication.
[91.] NSA/CSS Classification Guide, NSA, revised 1 April 1983.
[92.] "Rigging the game: Spy Sting", Tom Bowman, Scott Shane, *Baltimore Sun*, 10 December 1995.
[93.] "Wer ist der Befugte Vierte?", *Der Spiegel*, **36**, 1996, pp. 206-7.
[94.] "Secret Swedish E-Mail Can Be Read by the U.S.A", Fredrik Laurin, Calle Froste, *Svenska Dagbladet*, 18 November 1997.