DESENVOLVIMENTO DE TECNOLOGIAS DE VIGILÂNCIA E RISCO DE UTILIZAÇÃO ABUSIVA DE INFORMAÇÕES ECONÓMICAS

Vol. 2/5

A tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilíngues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz.

Documento de trabalho para o Painel STOA

Luxemburgo, Outubro de 1999 PE 168.184/Vol. 2/5

Dados para catalogação:

Título: **Parte 2/5:** A tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilíngues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz.

Ref. do plano de trabalho: EP/IV/B/STOA/98/1401

Publicação: Parlamento Europeu
Direcção-Geral de Estudos
Direcção A
Programa STOA

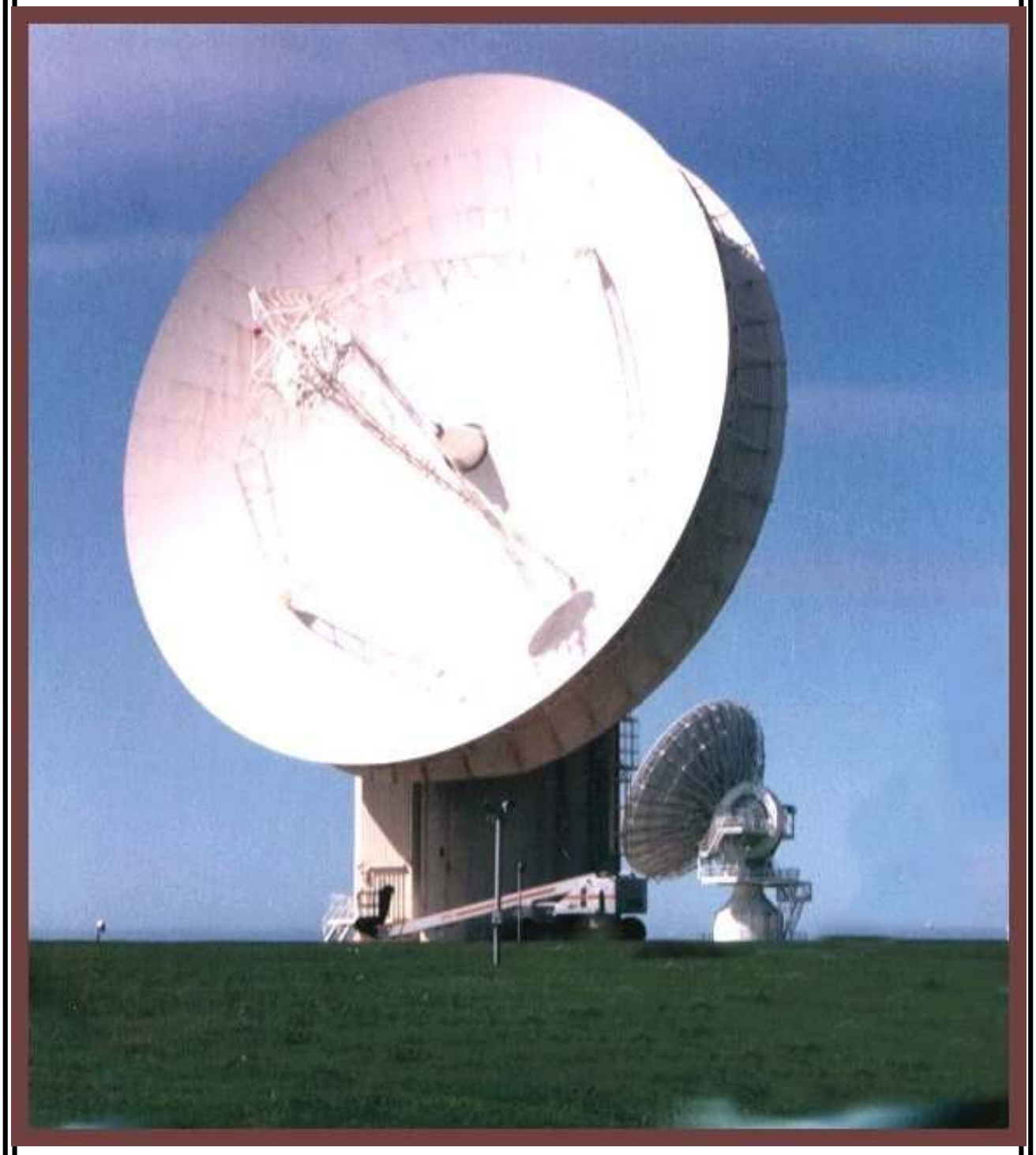
Autor: Duncan Campbell - IPTV Ltd. - Edimburgo

Editor: Dick HOLDSWORTH,
Chefe da Unidade STOA

Data: Outubro de 1999

Número PE: **PE 168.184 Vol. 2/5**

Capacidades de intercepção em 2000



Relatório destinado ao Director Geral de Estudos do Parlamento Europeu (gabinete do programa de avaliação das opções científicas e técnicas) relativamente ao desenvolvimento de tecnologias de vigilância e ao risco de utilização abusiva de informações económicas. Este estudo debruça-se sobre a tecnologia de ponta em matéria de espionagem de comunicações (COMINT) de processamento automatizado para fins de espionagem de sistemas, de operadores de rede pública ou alugada de banda larga multilíngues interceptados e a respectiva aplicabilidade na procura e selecção de COMINT, incluindo o reconhecimento de voz.

Capacidades de intercepção em 2000

Índice

Duncan Campbell
IPTV Ltd.
Edimburgo, Escócia
Abril de 1999

E-mail: iptv@cwcom.net

Capa: Antenas de 30 metros na estação da Composite Signals Organisation em Morwenstow, Inglaterra, que interceptam comunicações provenientes de satélites regionais no Oceano Atlântico e no Oceano Índico. (D. Campbell)

Resumo

1. A **espionagem de comunicações** (Comunications Intelligence - Comint), que envolve a intercepção secreta de comunicações estrangeiras, tem sido praticada por quase todas as nações avançadas desde existem telecomunicações internacionais. A Comint é uma actividade industrial em grande escala que fornece aos consumidores informações sobre desenvolvimentos diplomáticos, económicos e científicos. As capacidades e as limitações da actividade de Comint podem ser utilmente apreciadas no quadro do "ciclo de espionagem" (secção 1).

2. Globalmente, gastam-se por ano cerca de 15 a 20 mil milhões de Euros em Comint e actividades relacionadas. A maior parte destas despesas é realizada pelas principais nações de língua oficial inglesa da aliança UKUSA.[1] Este relatório descreve os métodos utilizados pelas organizações de Comint durante mais de 80 anos, para acederem à maioria das comunicações internacionais em todo o mundo. Estes métodos incluem a intercepção não autorizada de transmissões de satélites comerciais, de comunicações de longa distância provenientes do espaço, de cabos submarinos (utilizando submarinos) e da Internet. Existem mais de 120 sistemas de intercepção que actuam em simultâneo (secção 2).

3. O sistema UKUSA, altamente automatizado, com vista ao processamento de Comint, conhecido vulgarmente por ECHELON, tem sido muito debatido na Europa, no seguimento de um relatório do STOA em 1997.[2] Esse relatório resumia as informações provenientes das duas únicas fontes importantes disponíveis na altura sobre o ECHELON[3] e fornece documentação original nova e outras provas sobre a existência do sistema ECHELON e o seu envolvimento na intercepção de transmissões de satélites de telecomunicações (secção 3). Um anexo técnico fornece uma descrição suplementar pormenorizada sobre os métodos de processamento de Comint.

4. A informação Comint obtida a partir da intercepção de comunicações internacionais já há muito tempo que é habitualmente utilizada para obter dados delicados relativos a indivíduos, a governos e a organizações comerciais e internacionais. Este relatório estabelece os quadros de organização e de informação no âmbito dos quais os dados sensíveis do ponto de vista económico são recolhidos e divulgados, resumindo exemplos de organizações comerciais europeias que foram objecto de vigilância (secção 4).

5. Este relatório identifica uma organização internacional anteriormente desconhecida, "ILETS (Seminário Internacional sobre a Vigilância Legal das Telecomunicações)", que, sem qualquer discussão parlamentar ou pública e sem qualquer sensibilização, pôs em prática planos contenciosos que exigem que os fabricantes e operadores de novos sistemas de comunicações criem dispositivos de controlo que possam ser utilizados por organizações de segurança nacional ou de aplicação da lei (secção 5).

6. As organizações de Comint percebem agora que as dificuldades técnicas da intercepção de comunicações estão a aumentar e que a produção futura poderá ser mais onerosa e mais limitada do que actualmente. A percepção dessas dificuldades poderá constituir uma base útil para as opções políticas com vista a medidas de protecção relativas a informações económicas e a operações de criptagem eficazes (secção 6).

7. **Principais conclusões** relativas à tecnologia de ponta em Comint:

   - Existem sistemas globais para facultar acesso, interceptar e processar todas as formas modernas importantes de comunicação, com poucas excepções (secção 2, anexo técnico);
   - Contrariamente a informações veiculadas na imprensa, apesar de 30 anos de pesquisa, não existem ainda sistemas eficazes de "detecção de palavras" que seleccionem automaticamente chamadas telefónicas de interesse para a espionagem. Contudo, foram desenvolvidos sistemas de reconhecimento do orador - com efeito, "perfil vocal" - que estão prontos a reconhecer a voz de indivíduos definidos como alvo que façam telefonemas internacionais;
   - Recentes iniciativas diplomáticas por parte do governo dos Estados Unidos, procurando o acordo da Europa relativamente ao sistema de criptografia de "depósito de chave", ocultavam desígnios de recolha secreta de informações e faziam parte de um programa a longo prazo que violou, e continua a violar, a privacidade das comunicações de cidadãos não nacionais nos Estados Unidos, incluindo governos, empresas e cidadãos europeus;
   - Existem muitas provas que indicam que os principais governos efectuam, com carácter rotineiro, actividades de espionagem de comunicações para possibilitar vantagens comerciais às empresas e ao comércio em geral.

1. Organizações e métodos

O que é a espionagem de comunicações?

1. A espionagem de comunicações (Comint) encontra-se definida pela NSA, a maior agência que leva a cabo operações deste género, como "obtenção de informações" técnicas e secretas mediante intercepção de comunicações internacionais por outra pessoa que não o destinatário.[4] A Comint é uma das principais componentes da Sigint (espionagem de sinais), que também inclui a intercepção de sinais não respeitantes a comunicações, como as emissões de radar.[5] Embora este relatório refira agências e sistemas cuja tarefa global possa ser do âmbito da Sigint, diz respeito apenas a operações de Comint.

2. A Comint acompanhou o desenvolvimento de novos sistemas extensivos de telecomunicações civis de elevada capacidade e, consequentemente, tornou-se numa actividade industrial de grande escala, que dá emprego a muitos trabalhadores qualificados e utiliza níveis excepcionalmente elevados de automatização.

3. Os alvos das operações de Comint são variados. Os mais tradicionais são as mensagens militares e as comunicações diplomáticas entre capitais nacionais e as missões no estrangeiro. Desde os anos 60, no seguimento do crescimento do comércio mundial, a recolha de informações económicas secretas e de informações sobre desenvolvimentos científicos e técnicos tem sido um aspecto cada vez mais importante da Comint. Os alvos mais recentes incluem o tráfico de estupefacientes, a lavagem de dinheiro, o terrorismo e o crime organizado.

4. Sempre que se obtém acesso a canais de comunicações internacionais para uma finalidade, o acesso a todos os outros tipos de comunicações transportadas nos mesmos canais é automático, estando apenas sujeito à prioridade que as agências atribuam a cada tarefa. Assim, a NSA e o seu parceiro britânico, o GCHQ, por exemplo, utilizaram a Comint recolhida principalmente com outras finalidades para fornecer dados sobre figuras nacionais da oposição política nos Estados Unidos entre 1967 e 1975.

Aliança UKUSA

5. O United States Sigint System (USSS) é composto pela Agência de Segurança Nacional (NSA), unidades de apoio militar denominadas colectivamente de Central Security Service e partes da CIA e de outras organizações. Em 1947, no seguimento da colaboração em tempo de guerra, o Reino Unido e os EU assinaram um acordo secreto para continuarem a colaborar em actividades globais de Comint. Três outras nações de língua oficial inglesa, o Canadá, a Austrália e a Nova Zelândia, aderiram ao acordo UKUSA como "segundos contratantes". O acordo UKUSA só foi reconhecido publicamente em Março de 1999, quando o governo australiano confirmou que a respectiva organização de Sigint, a Defence Signals Directorate (DSD), cooperava com organizações de espionagem de sinais no estrangeiro, no âmbito da relação UKUSA.[6] O acordo UKUSA permite que instalações, tarefas e produtos sejam partilhados entre os governos participantes.

6. Embora o número de funcionários e os orçamentos da agência de Comint da UKUSA tenham diminuído a seguir ao final da "guerra fria", conseguiram reafirmar as suas exigências de acesso a todas as comunicações mundiais. Dirigindo-se ao pessoal da NSA aquando da sua partida em 1992, o então director da NSA, Almirante William Studeman, referiu que a procura de um maior acesso global estava em crescimento. A "área comercial" do "acesso global" era, segundo o Almirante, um dos dois pilares fortes – esperava ele -,sobre os quais a NSA deveria assentar no próximo século.[7]

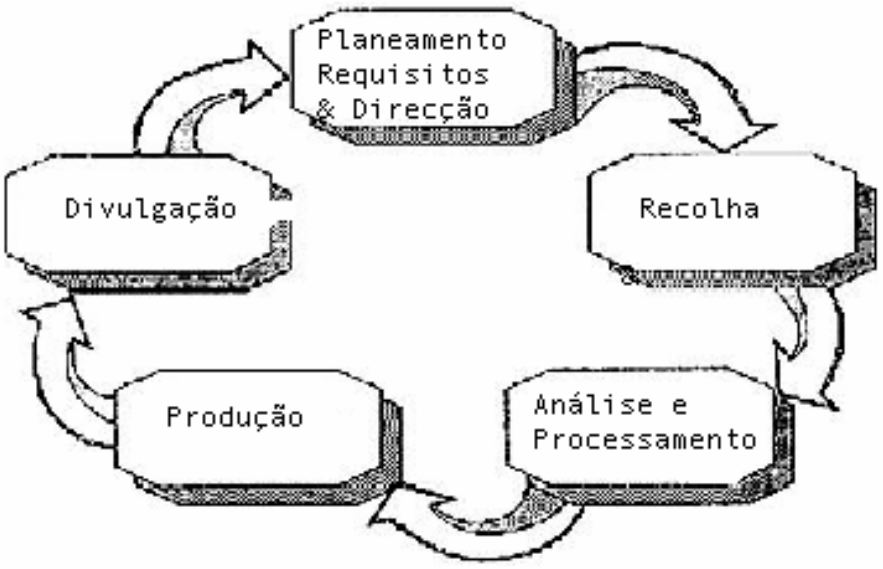
Outras organizações de Comint

7. Para além da UKUSA, existem, pelo menos, outras 30 nações que possuem importantes organizações de Comint em funcionamento. A maior destas é a FAPSI russa, com 54.000 funcionários.[8] A China mantém um sistema de Sigint substancial, no qual duas estações estão orientadas para a Rússia e funcionam em colaboração com os Estados Unidos. A maioria das nações do Médio Oriente e da Ásia investiram substancialmente em Sigint, em especial Israel, a Índia e o Paquistão.

Como funciona a espionagem

8. Depois da "guerra fria", a intercepção de Comint tem sido limitada por questões de carácter industrial, incluindo a necessidade de fazer corresponder os orçamentos e as capacidades às exigências dos clientes. O processo em várias etapas através do qual se procuram, recolhem, processam e passam informações secretas é semelhante em todos os países e é frequentemente descrito como o "ciclo de espionagem". As etapas do ciclo de informação correspondem a diferentes características técnicas e organizacionais da produção de Comint. Assim, por exemplo, a administração da maior estação da NSA no mundo, em Menwith Hill, Inglaterra, responsável pelo funcionamento de mais de 250 projectos secretos, encontra-se dividida em três direcções: OP, operações e planos; CP, processamento da recolha; e EP, exploração e produção.

INTELLIGENCE CYCLE



Planeamento

9. O planeamento envolve, em primeiro lugar, a determinação das exigências do cliente. Entre os clientes, contam-se os principais ministérios do governo patrocinador - nomeadamente aqueles que dizem respeito à defesa, aos negócios estrangeiros, à segurança, ao comércio e aos assuntos internos. A gestão global de Comint envolve a identificação das necessidades de dados, bem como a tradução das necessidades em tarefas potencialmente exequíveis, definição de prioridades, elaboração de análises e relatórios e controlo da qualidade do produto Comint.

10. Depois de seleccionados os objectivos, poderão ser **definidas tarefas** para as capacidades específicas de recolha, existentes ou novas, com base no tipo de informação necessária, na facilidade que o objectivo seleccionado ofereça para a recolha e na probabilidade de se obter uma recolha com interesse.

Acesso e recolha

11. O primeiro elemento essencial da Comint é o **acesso** ao meio de comunicação pretendido, para que as comunicações possam ser interceptadas. Historicamente, quando se utilizavam comunicações por rádio de longo alcance, esta tarefa era simples. Alguns importantes sistemas modernos de comunicação não facilitam a Comint e pode ser necessário utilizar métodos invulgares, onerosos ou intrusivos para se obter acesso aos mesmos. O meio físico de comunicação é normalmente independente do tipo de informação transportada. Por exemplo, os sistemas retransmissores de feixes hertzianos inter-cidades, as ligações internacionais via satélite e os cabos submarinos de fibra óptica transportarão normalmente um tráfego misto de sinais de televisão, telefone, fax, ligações de dados e voz, vídeo e dados privados.

12. A **recolha** segue-se à **intercepção**, mas é uma actividade distinta na medida em que podem ser interceptados muitos tipos de sinais, mas estes não receberão nenhum processamento adicional, excepto talvez as buscas técnicas para assegurar que os padrões das comunicações permaneçam inalterados. Por exemplo, uma estação de intercepção de satélites encarregada de estudar um satélite de comunicações recentemente lançado terá uma antena para interceptar tudo o que o satélite envia para o solo. Assim que um estudo tiver estabelecido quais as partes dos sinais do satélite que transportam, digamos, televisão ou comunicações sem qualquer interesse, a análise destes sinais é abandonada.

13. A recolha inclui a aquisição de informação através da intercepção e a transmissão das informações de interesse a jusante para que sejam **processadas** e **produzidas**. Devido às elevadas taxas de informação utilizadas em muitas redes modernas e à complexidade dos sinais nelas existentes, é agora comum que gravadores de alta velocidade ou memórias "instantâneas" retenham temporariamente grandes

quantidades de dados enquanto ocorre o processamento. As actividades de recolha modernas utilizam comunicações seguras e rápidas para transmitir dados através de redes globais para analistas humanos que podem estar noutro continente. A selecção das mensagens para a recolha e o processamento é, na maioria dos casos, automatizada, envolvendo grandes bancos de dados em linha que retêm informações sobre objectivos de interesse.

Processamento

14. O processamento é a conversão das informações recolhidas numa forma adequada, para análise ou produção de informação secreta, quer automaticamente quer sob supervisão humana. As comunicações recebidas são normalmente convertidas em formatos padrão que identificam as suas características técnicas, em conjunto com informações (tais como os números de telefone dos intervenientes numa conversa telefónica) relacionadas com a mensagem (ou sinal).

15. Numa fase inicial, caso não esteja inerente na selecção da mensagem ou conversa, cada sinal ou canal interceptado será descrito em "notação por caso" normal. Esta identifica primeiramente os países cujas comunicações foram interceptadas, normalmente através de duas letras. Uma terceira letra designa a classe geral das comunicações: C para intercepções de operadores de redes comerciais, D para mensagens diplomáticas, P para canais da polícia, etc.. Uma quarta letra designa o tipo de sistema de comunicação (como S para multi-canal). Depois, utilizam-se números que designam ligações ou redes específicas. Por exemplo, durante os anos 80, a NSA interceptou e processou tráfego designado por "FRD" (diplomático francês) a partir de Chicksands, em Inglaterra, enquanto a agência britânica de Comint GCHQ decifrou mensagens "ITD" (diplomáticas italianas) no seu quartel-general de Cheltenham.[9]

16. O processamento pode também envolver a tradução ou "síntese" (substituição de um texto integral pelo seu sentido ou por pontos principais de uma comunicação). A tradução e a síntese podem, até certo ponto, ser automáticos.

Produção e divulgação

17. A **produção** de Comint envolve a análise, avaliação, tradução e interpretação de dados não processados para obtenção da informação secreta final. A etapa final do ciclo de espionagem é a **divulgação**, que significa a passagem de relatórios aos consumidores de informação secreta. Esses relatórios podem ser compostos por mensagens não processadas (mas decifradas e/ou traduzidas), sínteses, comentários ou análises extensivas. A qualidade e a relevância dos relatórios divulgados levam, por seu turno, à redefinição das prioridades de recolha de informação, completando dessa forma o ciclo de espionagem.

18. A natureza da divulgação é altamente significativa para as questões relativas à forma como a Comint é explorada com vista à obtenção de vantagens económicas. As actividades de Comint em todo o mundo são altamente secretas porque, afirma-se, o conhecimento do sucesso da intercepção provavelmente levaria a que os alvos mudassem os seus métodos de comunicação para evitar futuras intercepções. No sistema UKUSA, a divulgação de relatórios de Comint é limitada a indivíduos que possuam autorizações de alto nível de segurança "SCI".[10] Para além disso, como apenas funcionários autorizados podem ver relatórios de Comint, só estes podem

definir os requisitos e, consequentemente, controlar a definição de tarefas. Os empregados de empresas comerciais normalmente não têm autorização nem acesso a Comint e, por isso, só poderão beneficiar de informações de Comint comercialmente relevantes na medida em que funcionários superiores do governo devidamente autorizados o permitam. Na Secção 5, mais adiante, descreve-se o procedimento que se segue nestes casos.

19. A divulgação é ainda mais limitada no seio da organização UKUSA por normas nacionais e internacionais que estipulam, de uma maneira geral, que as agências de Sigint de cada país não podem normalmente recolher nem (se recolhidas inadvertidamente) gravar ou divulgar informações acerca de cidadãos ou empresas com domicílio em qualquer outro país do acordo UKUSA. Os cidadãos e as empresas são colectivamente denominados como "pessoas jurídicas". Se a pessoa em causa tiver sido objecto de vigilância da respectiva organização nacional de Comint, é seguido o procedimento contrário.

20. Por exemplo, Hager descreveu[11] o modo como funcionários neozelandeses receberam instruções para retirar dos seus relatórios os nomes de cidadãos ou empresas da UKUSA identificáveis, inserindo, em substituição, palavras como "um cidadão canadiano" ou "uma empresa norte-americana". Os funcionários da organização de Comint britânica afirmaram seguir procedimentos semelhantes no que diz respeito aos cidadãos dos Estados Unidos, no seguimento da introdução de legislação para limitar as actividades de espionagem interna da NSA em 1978.[12] O Governo australiano afirma que o DSD e os seus pares possuem procedimentos internos para se satisfazerem com o facto de os seus interesses e políticas nacionais serem respeitados pelos outros. [...] As regras (relativas à Sigint e aos australianos) proíbem a divulgação de informações relativas a pessoas australianas, obtidas acidentalmente no decorrer da recolha rotineira de comunicações estrangeiras, ou o registo e a notificação dos nomes das pessoas australianos mencionadas nessas comunicações.[13] O corolário é também verdadeiro: os países UKUSA não colocam quaisquer restrições à recolha de informação secreta que afecte cidadãos ou empresas de qualquer país não pertencente à UKUSA, incluindo os Estados-Membros da União Europeia (à excepção do Reino Unido).

2. Intercepção de comunicações internacionais

Comunicações por operadores internacionais de redes alugadas (ILC)

21. Deve registar-se que as comunicações estrangeiras com destino e proveniência ou passagem pelo Reino Unido e pelos Estados Unidos são interceptadas há mais de 80 anos.[14] Na altura, e desde então, a maior parte das ligações de comunicações internacionais têm sido realizadas por operadores internacionais, tratando-se normalmente de empresas públicas nacionais de telecomunicações ou empresas privadas. Em qualquer dos casos, a capacidade do sistema de comunicação é alugada a empresas nacionais ou internacionais de telecomunicações. Por este motivo, as organizações de Comint utilizam o termo ILC (International Leased Carrier) para descrever este tipo de recolha.

Rádio de alta frequência

22. À excepção das ligações terrestres directas entre nações geograficamente contíguas, o sistema de rádio de alta frequência (HF) era o meio mais comum para as telecomunicações internacionais antes de 1960 e era utilizado para fins de ILC, diplomáticos e militares. Uma característica importante dos sinais de rádio de HF é que estes são reflectidos a partir da ionoesfera e a partir da superfície terrestre, facultando um alcance de milhares de quilómetros. Isto permite tanto a recepção como a intercepção.

Feixes hertzianos

23. Os feixes hertzianos foram introduzidos nos anos 50 para proporcionar comunicações inter-cidades de grande capacidade para a telefonia, a telegrafia e, mais tarde, a televisão. As comunicações por feixes hertzianos utilizam transmissores de baixa potência e antenas parabólicas colocadas em torres em posições elevadas, tais como no topo de montanhas ou de edifícios altos. As antenas têm, geralmente, um diâmetro de 1 a 3 metros. Devido à curvatura da terra, são normalmente necessárias estações de retransmissão a cada 30 - 50 Km.

Cabos submarinos

24. Os cabos telefónicos submarinos proporcionaram os primeiros grandes sistemas de comunicações internacionais de elevada capacidade e fiáveis. Os sistemas iniciais limitavam-se a algumas centenas de canais telefónicos simultâneos. Os sistemas de fibra óptica mais modernos transportam até 5 Gbps (Gigabits por segundo) de informações digitais. Isto é aproximadamente equivalente a cerca de 60.000 canais telefónicos simultâneos.

Satélites de telecomunicação

25. Os sinais dos feixes hertzianos não são reflectidos pela ionoesfera e passam directamente para o espaço. Esta propriedade foi explorada para facultar comunicações globais e, por outro lado, para interceptar este tipo de comunicações no espaço e na terra. A maior constelação de satélites de comunicação (COMSATs) é explorada pela Organização Internacional de Telecomunicações por Satélite (Intelsat),

uma organização de tratado internacional. Para que sejam fornecidas comunicações permanentes de ponto a ponto ou para fins de difusão, os satélites de comunicação são colocados nas denominadas órbitas "geoestacionárias" de forma a que, para o observador na Terra, pareçam manter sempre a mesma posição no céu.

26. Os primeiros satélites geoestacionários da Intelsat foram colocados em órbita em 1967. A tecnologia dos satélites desenvolveu-se rapidamente. A quarta geração de satélites da Intelsat, introduzida em 1971, fornecia capacidade para 4.000 canais telefónicos simultâneos e era capaz de lidar em simultâneo com todas as formas de comunicação - telefone, telex, telégrafo, televisão, dados e facsmile. Em 1999, a Intelsat tinha em funcionamento 19 satélites das suas 5ª a 8ª gerações. A última geração pode lidar com o equivalente a 90.000 telefonemas simultâneos.

Técnicas de telecomunicação

27. Antes de 1970, a maior parte dos sistemas de comunicação (independentemente da forma de transporte) utilizavam técnicas analógicas ou de onda contínua. Desde 1990, quase todas as comunicações se tornaram digitais, facultando uma capacidade cada vez maior. O sistema de maior capacidade utilizado em geral para a Internet, denominado STM-1 ou OC-3, funciona a uma velocidade de 155 Mbs (milhão de bits por segundo; uma velocidade de 155 Mbs é equivalente ao envio de 3 milhões de palavras por segundo, praticamente o texto de mil livros por minuto). Por exemplo, são utilizadas ligações com esta capacidade para estabelecer ligações através da infra-estrutura da Internet entre a Europa e os Estados Unidos. No anexo técnico são fornecidos pormenores adicionais sobre as tecnologias de comunicação.

Recolha de comunicações por ILC

Acesso

28. A recolha de Comint só pode ocorrer se a agência de recolha obtiver acesso aos canais de comunicação que deseja examinar. As informações sobre os meios utilizados para a obtenção do acesso são, tal como os dados sobre métodos de descodificação, as informações mais protegidas em qualquer organização de Comint. O acesso é obtido com e sem a cumplicidade ou cooperação dos operadores das redes.

Operação SHAMROCK

29. A partir de 1945, nos Estados Unidos, a NSA e as agências predecessoras obtinham sistematicamente tráfego por cabo proveniente dos escritórios dos principais operadores por cabo. Esta actividade tinha o nome de código SHAMROCK e permaneceu secreta durante 30 anos, até que foram reveladas pelos inquéritos ao caso Watergate. A 8 de Agosto de 1975, o director da NSA Tenente General Lew Allen admitiu ao Comité Pike da Câmara dos Representantes dos Estados Unidos que a *NSA interceptava sistematicamente comunicações internacionais, tanto de voz como por cabo*.

Antena de intercepção de rádio de alta frequência (AN/FLR9)

Tabuleta do DODJOCC na estação da NSA, Chicksands

30. Admitiu também que tinham sido recolhidas mensagens enviadas e recebidas por cidadãos americanos no decurso da intercepção de comunicações internacionais. Os legisladores norte-americanos consideraram que estas operações poderão ter sido inconstitucionais. Em 1976, uma equipa do Departamento de Justiça investigou possíveis crimes efectuados pela NSA. Parte do seu relatório foi publicada em 1980, descrevendo a forma como as informações sobre cidadãos norte-americanos era *obtida acidentalmente, no decurso da intercepção, por parte da NSA, de comunicações internacionais orais ou não (por exemplo, telex) e da recepção de tráfego de telex e de ILC por cabo (SHAMROCK), adquirido pelo GCHQ.*[15]

Intercepção de sinais de rádio de alta frequência

31. Os sinais de rádio de alta frequência são relativamente fáceis de interceptar, necessitando apenas de uma área adequada de terreno num ambiente de rádio idealmente "sossegado". De 1945 até ao início dos anos 80, tanto a NSA como o GCHQ possuíam sistemas de intercepção de rádio de HF com a missão de recolher comunicações de ILC europeias na Escócia.[16]

32. O tipo mais avançado de sistema de monitorização de HF utilizado neste período com vista a Comint foi um grande sistema de antenas circulares conhecido como AN/FLR-9. As antenas do sistema AN/FLR-9 têm um diâmetro superior a 400 metros. Podem interceptar e simultaneamente determinar a existência de sinais de tantas direcções e em tantas frequências quantas as que se desejar. Em 1964, foram instalados sistemas de recepção AN/FLR-9 em San Vito dei Normanni, Itália, em Chicksands, Inglaterra, em Karamursel, Turquia.

33. Em Agosto de 1966, a NSA transferiu as actividades de recolha de ILC das suas instalações escocesas em Kirknewton para Menwith Hill, em Inglaterra. Dez anos mais tarde, esta actividade foi novamente transferida, desta feita para Chicksands. Embora a função principal das instalações de Chicksands fosse interceptar comunicações da força aérea soviética e do Pacto de Varsóvia, tinham também a missão de recolher ILC e "NDC" (comunicações diplomáticas não norte-americanas). Proeminente entre estas tarefas era a recolha de tráfego FRD (ou seja, comunicações diplomáticas francesas). Embora a maior parte dos funcionários em Chicksands fossem membros da Força Aérea dos Estados Unidos, a intercepção de comunicações diplomáticas e de ILC era tratada por funcionários civis da NSA numa unidade denominada DODJOCC.[17]

34. Durante a década de 1970, as unidades de Comint britânicas no Chipre tiveram a missão de recolher comunicações em HF de nações aliadas da NATO, incluindo a Grécia e a Turquia. A intercepção ocorria numa unidade do exército britânico em Ayios Nikolaos, no leste do Chipre.[18] Em 1975, nos Estados Unidos, as investigações realizadas por um Comité do Congresso revelaram que a NSA recolhia mensagens diplomáticas enviadas de e para Washington, numas instalações de Comint do exército em Vint Hill Farms, Virgínia. Os alvos desta estação incluíam o Reino Unido.[19]

Intercepção no espaço de redes inter-cidades

35. As ligações por feixes hertzianos de longa distância podem necessitar de dúzias de estações intermédias para receber e retransmitir as comunicações. Cada estação de recepção subsequente recebe apenas uma minúscula fracção do sinal originalmente transmitido, passando o restante sobre o horizonte, em direcção ao espaço, onde os satélites o podem recolher. Estes princípios foram explorados durante a década de 1960 de forma a facultar a recolha de Comint a partir do espaço. A natureza destes "derrames" de microondas significa que a melhor posição para esses satélites não é acima do alvo escolhido, mas a uma distância de até 80 graus de longitude.

36. O primeiro satélite de Comint dos Estados Unidos, o CANYON, foi lançado em Agosto de 1968, sendo em breve seguido por um outro. Os satélites eram controlados a partir de uma estação terrestre em Bad Aibling, na Alemanha. De forma a facultar uma cobertura permanente dos alvos seleccionados, os satélites CANYON eram colocados junto a órbitas geoestacionárias. Contudo, as órbitas não eram exactas, fazendo com que os satélites mudassem de posição e obtivessem mais dados relativamente a alvos no solo.[20] Foram lançados sete satélites CANYON entre 1968 e 1977.

Torre de feixes hertzianos inter-cidades "derrama" os seus sinais para o espaço

37. O alvo do CANYON era a União Soviética. As principais ligações soviéticas de comunicações estendiam-se por milhares de quilómetros, em grande parte sobre a Sibéria, onde os gelos permanentes limitavam a utilização fiável de cabos subterrâneos. Assim sendo, as circunstâncias geográficas favoreciam a NSA pois tornavam as ligações de comunicação interna da União Soviética altamente acessíveis. Os satélites tinham um desempenho superior ao esperado, pelo que o projecto foi alargado.

38. O sucesso do CANYON levou à concepção e utilização de uma nova classe de satélites de Comint, os CHALET. A estação terrestre escolhida para a série CHALET foi Menwith Hill, em Inglaterra. No âmbito do projecto P-285 da NSA, foram contratadas empresas norte-americanas para instalar e auxiliar na operação do sistema de controlo dos satélites e das ligações descendentes (RUNWAY), bem como do sistema de processamento no solo (SILKWORTH). Os dois primeiros satélites CHALET foram lançados em Junho de 1978 e Outubro de 1979. Após o nome do primeiro satélite ter aparecido na imprensa norte-americana, foi-lhes atribuído o novo nome de VORTEX. Em 1982, a NSA obteve a aprovação para “novos requisitos de missão” mais abrangentes e recebeu financiamento e instalações para trabalhar simultaneamente com quatro satélites VORTEX. Foi construído um novo centro de operações com 5.000 m² (STEEPLEBUSH) foi construído para albergar o equipamento de processamento. Quando o nome VORTEX foi publicado em 1987, o nome dos satélites foi novamente alterado, desta vez para MERCURY.[21]

39. A missão alargada dada a Menwith Hill, após 1985, incluía a recolha de informação do Médio Oriente através dos satélites MERCURY. A estação recebeu um prémio pelo apoio prestado às operações navais norte-americanas no Golfo Pérsico entre 1987 e 1988. Em 1991, recebeu mais um prémio pelo apoio prestado às operações Tempestade no Deserto e Escudo do Deserto, na guerra contra o Iraque.[22] Menwith Hill é agora a principal unidade norte-americana de recolha de Comint contra o seu maior aliado, Israel. O seu quadro de pessoal inclui linguistas especializados em hebraico, árabe e farsi, bem como em línguas europeias. Menwith Hill foi recentemente ampliada de forma a incluir ligações terrestres para um nova rede de satélites Sigint lançada em 1994 e 1995 (RUTLEY). O nome desta nova classe de satélites é ainda desconhecido.

Satélites Sigint

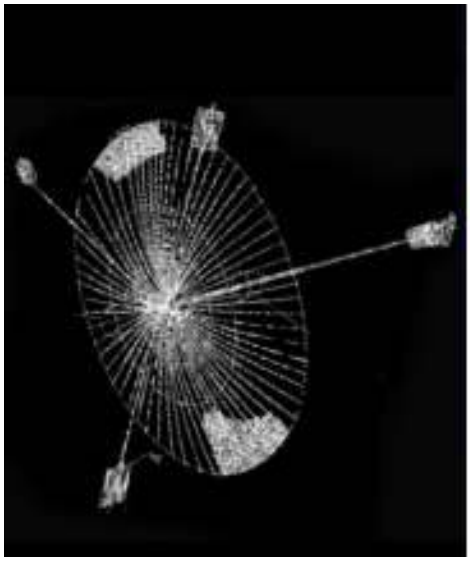
40. A CIA desenvolveu uma segunda classe de satélites Sigint com capacidades complementares, no período de 1967 a 1985. Inicialmente conhecidos como RHYOLITE e, posteriormente, como AQUACADE, estes satélites eram operados a partir de uma estação terrestre remota no centro da Austrália, em Pine Gap. Utilizando uma grande antena parabólica que se desdobrava no espaço, os satélites RHYOLITE

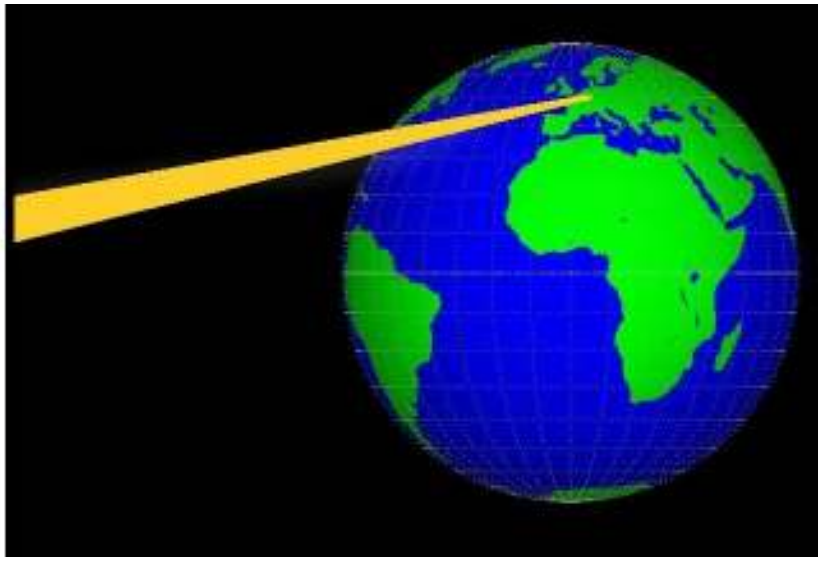
interceptavam sinais de frequência mais baixa nas bandas VHF e UHF. A satélites maiores e mais recentes deste tipo foi atribuído o nome MAGNUM e depois ORION. Os seus alvos incluem a telemetria, rádio VHF, telemóveis, sinais de aparelhos de chamada de pessoas e ligações de dados móveis.

41. Uma terceira classe de satélites, conhecida primeiro como JUMPSEAT e posteriormente como TRUMPET, trabalha em órbitas altamente elípticas e quase polares, o que lhes permite "pairar" durante muito tempo sobre latitudes setentrionais elevadas. Estes satélites permitem que os Estados Unidos recolham sinais de transmissores em latitudes setentrionais elevadas que não são bem abrangidas pelos satélites MERCURY ou ORION e também interceptar sinais enviados para satélites de comunicação russos nas mesmas órbitas.

42. Embora os pormenores precisos sobre os satélites Sigint dos Estados Unidos lançados após 1990 permaneçam obscuros, é evidente, a partir da observação de centros terrestres relevantes, que os sistemas de recolha se expandiram em vez de diminuírem. As principais estações encontram-se em Buckley Field (Denver, Colorado), Pine Gap (Austrália), Menwith Hill (Inglaterra) e Bad Aibling (Alemanha). Os satélites e as respectivas unidades de processamento são excepcionalmente dispendiosos (na ordem dos mil milhões de dólares americanos cada). Em 1998, a Organização Nacional de Reconhecimento (National Reconnaissance Office-NRO) anunciou planos para combinar as três classes distintas de satélites Sigint numa arquitectura de Sigint aérea integrada (Integrated Overhead Sigint Architecture - IOSA), de forma a melhorar o desempenho da Sigint e evitar os custos através da consolidação de sistemas, utilizando novas tecnologias de satélites e de processamento de dados.[23]

43. O que se segue é que, dentro das limitações impostas pelos orçamentos e pelas prioridades na definição de tarefas, os Estados Unidos podem, caso o desejem, orientar os sistemas de recolha no espaço para que interceptem sinais de comunicações móveis e tráfego de microondas inter-cidades em qualquer ponto do planeta. As dificuldades geográficas e de processamento na recolha de mensagens de todas as partes do globo em simultâneo, sugerem veementemente que a definição de tarefas para estes satélites será orientada para os alvos nacionais e militares de maior prioridade. Consequentemente, embora as comunicações europeias que passam em rotas de microondas inter-cidades possam ser recolhidas, é provável que sejam normalmente ignoradas. Mas é altamente provável que as comunicações para a Europa ou dela provenientes e que passem pelas redes de comunicação por microondas dos Estados do Médio Oriente sejam recolhidas e processadas.





Satélites de Comint em órbitas geoestacionárias, como os VORTEX, interceptam "derrames" de microondas na terra.

44. Nenhuma outra nação (incluindo a ex-União Soviética) utilizou satélites comparáveis ao CANYON, ao RHYOLITE ou aos seus sucessores. Tanto a Grã-Bretanha (projecto ZIRCON) como a França (projecto ZENON) tentaram fazê-lo, mas nenhuma conseguiu. Depois de 1988, o governo britânico adquiriu capacidades na constelação VORTEX norte-americana (agora MERCURY) para fins nacionais unilaterais.[24] Um oficial de ligação do Reino Unido e funcionários do GCHQ trabalham na estação da NSA em Menwith Hill e ajudam na definição de tarefas e na operação dos satélites.

Intercepção de COMSAT efectuados por ILC

45. A recolha sistemática de comunicações COMSAT efectuados por ILC começou em 1971. Foram construídas duas estações terrestres para esta finalidade. A primeira, em Morwenstow, na Cornualha, Inglaterra, tinha duas antenas de 30 metros. Uma interceptava comunicações provenientes do Intelsat no Oceano Atlântico, a outra do Intelsat no Oceano Índico. O segundo local de intercepção Intelsat situava-se em Yakima, Washington, no noroeste dos Estados Unidos. A estação de investigação de Yakima da NSA interceptava comunicações que passassem pelos satélites Intelsat no Oceano Pacífico.

46. A capacidade de intercepção de ILC contra satélites de comunicações operados pelo Ocidente permaneceu a este nível até ao final da década de 1970, quando uma segunda unidade norte-americana em Sugar Grove, Virgínia Ocidental foi adicionada à rede. Em 1980, as suas três antenas de satélites tinham sido cedidas ao Naval Security Group dos Estados Unidos e foram utilizadas para a intercepção de COMSAT. A expansão em grande escala do sistema de intercepção de satélites de ILC decorreu entre 1985 e 1995, em conjunto com o alargamento do sistema de processamento ECHELON (secção 3). Foram construídas novas estações nos Estados Unidos (Sabana Seca, Porto Rico), no Canadá (Leitrim, Ontário), na Austrália (Kojarena, Austrália Ocidental) e na Nova Zelândia (Waihopai, Ilha do Sul). A capacidade em Yakima, Morwenstow e Sugar Grove foi aumentada e continua a aumentar.

Numa simples contagem do número de antenas actualmente instaladas em cada estação de intercepção de COMSAT ou de satélites Sigint, parece indicar que **as nações UKUSA, entre si, operam actualmente pelo menos 120 sistemas de recolha com base em satélites**. O número aproximado de antenas em cada categoria é o seguinte:

- **orientados para satélites de comunicações comerciais ocidentais (ILC)**	**40**
- **a controlar satélites de espionagem de sinais com base no espaço**	**30**
- **actualmente ou anteriormente orientados para satélites de comunicações soviéticos**	**50**

Os sistemas da terceira categoria podem ter sido colocados em tarefas de ILC desde o final da "guerra fria".[25]

47. Outras nações recolhem, cada vez mais, Comint a partir de satélites. A FAPSI russa possui grandes unidades terrestres de recolha em Lourdes, Cuba e em Cam Ranh Bay, no Vietname.[26] Alegadamente, a BND alemã e a DGSE francesa colaboram na operação de uma unidade de recolha de COMSAT em Kourou, Guiana, cujo alvo são

as comunicações norte-americanas e sul-americanas via satélite. Também se afirma que a DGSE possui unidades de recolha de COMSAT em Domme (Dordogne, França), na Nova Caledónia e nos Emirados Árabes Unidos.[27] Os serviços secretos suíços anunciaram recentemente um plano para duas estações de intercepção de COMSAT.[28]

Terminal terrestre de satélites em Etam, Virgínia Ocidental, que liga a Europa e os EUA através do Intelsat IV

O GCHQ construiu uma estação "sombra" idêntica, em 1972, para interceptar mensagens de Intelsat para a UKUSA

Intercepção de cabos submarinos

48. Os cabos submarinos desempenham agora um papel predominante nas telecomunicações internacionais, uma vez que, ao contrário da largura de banda limitada disponível nos sistemas espaciais, os meios ópticos proporcionam uma capacidade aparentemente ilimitada. Excepto nos casos em que os cabos terminam em países onde os operadores de telecomunicações fornecem o acesso a Comint (como o Reino Unido e os Estados Unidos), os cabos submarinos parecem ser intrinsecamente seguros devido à natureza do ambiente oceânico.

49. Em Outubro de 1971, provou-se que esta segurança era inexistente. Um submarino norte-americano, o Halibut, visitou o Mar de Okhotsk, ao largo da URSS oriental, e gravou comunicações que passavam num cabo militar para a Península de Khamchatka. O Halibut estava equipado com uma câmara de mergulho a grande profundidade, perfeitamente visível na popa do submarino. A câmara foi descrita pela Marinha norte-americana como um "veículo de salvamento a grande profundidade". A verdade é que o "veículo de salvamento" estava soldado ao submarino solidamente. Depois de submerso, mergulhadores de grande profundidade saíam do submarino e enrolavam bobines de escuta à volta do cabo. Tendo provado este princípio, o USS Halibut voltou em 1972 e colocou uma cápsula de gravação de alta capacidade junto ao cabo. A técnica não envolvia quaisquer danos físicos e era pouco provável que fosse rapidamente detectada.[29]

50. A operação de colocação de escutas em cabos em Okhotsk continuou durante dez anos, envolvendo viagens rotineiras por três submarinos diferentes, especialmente equipados para recolher as cápsulas antigas e colocar novas, por vezes mais do que uma cápsula de cada vez. Foram adicionados novos alvos em 1979. No Verão desse ano, um submarino recentemente convertido, o USS Parche, viajou de São Francisco, sob o Pólo Norte, até ao Mar de Barents e colocou uma nova escuta de cabo junto a Murmansk. A tripulação recebeu uma menção presidencial pelo seu feito. A colocação de escutas em cabos em Okhotsk terminou em 1982, após a respectiva localização ter sido comprometida por um antigo funcionário da NSA que vendeu informações acerca das escutas, cujo nome de código era IVY BELLS, à União Soviética. Uma das cápsulas IVY BELLS encontra-se agora em exposição no museu da antiga KGB em Moscovo. A operação de colocação de escutas no Mar de Barents continuou sem ser detectada até à sua interrupção em 1992.

51. Em 1985, as operações de colocação de escutas em cabos foram alargadas ao Mediterrâneo, para interceptar os cabos que faziam a ligação entre a Europa e a África Ocidental.[30] Depois do final da "guerra fria", o USS Parche foi reequipado com uma secção aumentada para poder acomodar equipamento e cápsulas de escuta de maiores dimensões. As escutas de cabos podiam ser colocadas por comando à distância, através de mecanismos telecomandados. O USS Parche continua em funcionamento, mas os alvos das suas missões permanecem desconhecidos. A administração de Clinton atribui, evidentemente, um elevado valor aos seus feitos. Todos os anos, entre 1994 e 1997, a tripulação do submarino foi altamente elogiada.[31] Os alvos prováveis podem incluir o Médio Oriente, o Mediterrâneo, a Ásia Oriental e a América do Sul. Os Estados Unidos são a única potência naval que se sabe ter utilizado tecnologias de grande profundidade para esta finalidade.

52. Foram também utilizados gravadores miniaturizados para escutas indutivas para interceptar cabos subterrâneos.[32] No entanto, os cabos de fibra óptica não têm perda de sinais de radiofrequência e não podem ser submetidos a escutas utilizando circuitos indutivos. A NSA e outras agências de Comint gastaram grandes quantidades de dinheiro em investigações sobre a colocação de escutas em fibras ópticas, sem grande sucesso. Mas os cabos de fibra óptica de longa distância não são invulneráveis. O principal meio de acesso é através da adulteração de "repetidores" opto-electrónicos que aumentam os níveis dos sinais em longas distâncias. O que acontece é que qualquer sistema de cabos submarinos que utilize repetidores opto-electrónicos submersos não pode ser considerado seguro contra actividades de intercepção e de espionagem de comunicações.

O USS Halibut com câmara de mergulho dissimulada

Cápsula de escuta colocada por submarino norte-americano ao largo de Khamchatka

Intercepção de comunicações da Internet

53. O forte crescimento na dimensão e importância da Internet e das formas associadas de comunicação digital coloca, segundo algumas pessoas, um desafio para as agências de Comint, o que não parece correcto. Durante a década de 1980, a NSA e os seus parceiros da UKUSA possuíam uma rede de comunicações internacionais maior do que a Internet de então, mas com base na mesma tecnologia.[33] Segundo o parceiro britânico, todos os sistemas do GCHQ estão interligados na maior LAN [rede de área local] da Europa, que está ligada a outros locais do mundo através de uma das maiores WAN [redes de área amplificada] do mundo. O seu principal protocolo de ligação em rede é o Protocolo Internet (IP).[34] Esta rede global, desenvolvida como projecto EMBROIDERY, inclui a PATHWAY, a principal rede de comunicações por computador da NSA, e faculta comunicações globais rápidas e seguras para o ECHELON e outros sistemas.

54. Desde o início dos anos 1990 foram desenvolvidos sistemas de Comint rápidos e sofisticados para recolher, filtrar e analisar as formas de comunicação digital rápida utilizadas pela Internet. Uma vez que a maior parte da capacidade mundial, em termos de Internet, se situa nos Estados Unidos ou está ligada aos Estados Unidos, muitas comunicações no "ciberespaço" passarão por sítios intermédios nos Estados Unidos. As comunicações provenientes da Europa com destino à Ásia, Oceânia, África ou América do Sul, ou provenientes destas, passam normalmente pelos Estados Unidos.

55. As rotas feitas pelos "pacotes" da Internet dependem da origem e do destino dos dados, dos sistemas através dos quais entram e saem da Internet e de inúmeros outros factores, incluindo a hora do dia. Consequentemente, os selectores de rotas na América ocidental estão no seu período mais inactivo quando o tráfego do centro da Europa está a chegar ao máximo da sua utilização. É assim possível (e razoável) que as mensagens que viajam uma curta distância numa rede europeia ocupada viajem, por exemplo, através dos intercâmbios da Internet na Califórnia. Uma grande proporção das comunicações internacionais na Internet passará assim, devido à natureza do sistema, através dos Estados Unidos, ficando facilmente acessíveis para a NSA.

56. As mensagens normais da Internet são compostas por pacotes denominados "datagramas". Os datagramas incluem números que representam a respectiva origem e destino, denominados "endereços de IP". Os endereços são exclusivos de cada computador ligado à Internet. São inerentemente fáceis de identificar no que diz respeito ao país e ao local de origem e de destino. O manuseamento, a triagem e o encaminhamento de milhões destes pacotes, por segundo, é fundamental para o funcionamento dos principais centros de Internet. O mesmo processo facilita a extracção de tráfego com vista à Comint.

57. O tráfego na Internet pode ser acedido a partir de ligações de comunicações internacionais que entrem nos Estados Unidos ou quando atinge os principais intercâmbios da Internet. Ambos os métodos possuem vantagens. O acesso aos sistemas de comunicação permanecerá, provavelmente, clandestino, enquanto o acesso aos intercâmbios da Internet poderá ser mais detectável, embora forneça um acesso mais fácil a mais dados e a métodos de triagem mais simples. Embora as quantidades de dados envolvidos sejam enormes, a NSA está normalmente limitada

por lei apenas às comunicações que tenham início ou fim num país estrangeiro. A não ser que sejam emitidos mandatos específicos, todos os outros dados deverão ser normalmente eliminados pelo equipamento antes que possam ser examinados e gravados.

58. Muito do outro tráfego na Internet (quer seja de fora dos Estados Unidos quer não) é de interesse comum em termos de informação secreta ou pode ser manuseado de formas diferentes. Por exemplo, as mensagens enviadas para grupos de discussão "Usenet" ascendem a cerca de 15 *Gigabytes* (Gb) de dados por dia, o equivalente a cerca de 10.000 livros. Todos estes dados são transmitidos a quem quiser (ou estiver disposto a) recebê-los. Tal como outros utilizadores da Internet, as agências de espionagem têm acesso aberto a estes dados, podendo armazená-los e analisá-los. No Reino Unido, a Agência de Investigação e Avaliação de Defesa (DERA) mantém uma base de dados de 1 *Terabyte* que contém as mensagens dos 90 dias anteriores da Usenet.[35] Um serviço semelhante, chamado "Deja News", está disponível para utilizadores da World Wide Web (WWW). As mensagens para a Usenet são facilmente distinguíveis. Não faz sentido recolhê-las clandestinamente.

59. Considerações semelhantes afectam a World Wide Web, a maior parte da qual é de acesso livre. Os sítios Web são examinados continuamente por "motores de busca" que geram catálogos dos seus conteúdos. "Alta Vista" e "Hotbot" são sítios públicos proeminentes neste género. A NSA emprega de forma semelhante "bots" (robots) para recolher dados de interesse. Por exemplo, um sítio Web nova-iorquino, conhecido como JYA.COM (http://www.jya.com/cryptome) oferece informações públicas alargadas sobre Sigint, Comint e criptografia. Este sítio é frequentemente actualizado. Os registos do acesso ao sítio mostram que todas as manhãs ele é visitado por um "bot" do National Computer Security Centre da NSA, que procura novos ficheiros e faz cópias de todos os que encontre.[36]

60. O que acontece é que o tráfego estrangeiro na Internet com interesse para a espionagem de comunicações (composto por mensagens de correio electrónico, transferências de ficheiros, "redes privadas virtuais" que funcionam na Internet e algumas outras mensagens) formarão, na melhor das hipóteses, uma pequena percentagem do tráfego nos principais intercâmbios da Internet ou principais ligações norte-americanas. Segundo um antigo funcionário, a NSA, em 1995, já tinha instalado *software* de detecção para recolher esse tipo de tráfego em nove dos principais pontos de intercâmbio da Internet (IXPs).[37] Os dois primeiros sítios deste género a ser identificados, o FIX East e o FIX West, são operados por agências governamentais dos Estados Unidos. Estão em estreita ligação com locais comerciais próximos, o MAE East e o MAE West (consultar quadro). Três outros sítios indicados eram pontos de acesso à rede (Network Acess Points), inicialmente desenvolvidos pela Fundação Nacional para a Ciência dos Estados Unidos para facultar à Internet norte-americana a sua "espinha dorsal" inicial.

Sítio da Internet	Localização	Operador	Designação
FIX East	College Park, Maryland	Governo dos Estados Unidos	Federal Information Exchange
FIX West	Mountain View, Califórnia	Governo dos Estados Unidos	Federal Information Exchange
MAE East	Washington, DC	MCI	Metropolitan Area Ethernet
New York NAP	Pennsauken, Nova Jérsia	Sprintlink	Network Acess Point
SWAB	Washington, DC	PSInet/Bell Atlantic	SMDS Washington Area Bypass
Chicago NAP	Chicago, Ilinóis	Ameritech/Bellcorp	Network Acess Point
San Francisco NAP	São Francisco, Califórnia	Pacific Bell	Network Acess Point
MAE West	São José, Califórnia	MCI	Metropolitan Area Ethernet
CIX	Santa Clara, Califórnia	CIX	Commercial Internet Exchange

Quadro 1. Acesso a Comint na Internet pela NSA em sítios IXP (1995)[38]

61. O mesmo artigo alegava que uma empresa norte-americana líder no campo da Internet e das telecomunicações tinha assinado um contrato com a NSA para desenvolver *software* para captar dados de interesse na Internet e que tinham sido feitos acordos com os fabricantes líderes Microsoft, Lotus e Netscape, para que alterassem os seus produtos para utilização no estrangeiro. Comprovou-se que esta última alegação estava correcta (consultar anexo técnico). O fornecimento destas funções não faria muito sentido a não ser que a NSA também tivesse conseguido um acesso geral ao tráfego da Internet. Embora a NSA não confirme nem negue estas alegações, um processo jurídico na Grã-Bretanha, em 1997, que envolvia uma alegada "pirataria informática" mostrou provas da vigilância feita pela NSA na Internet. Testemunhas da componente da Força Aérea norte-americana da NSA reconheceram utilizar detectores de pacotes e programas especiais para detectar tentativas de entrada nos computadores militares norte-americanos. O caso foi arquivado após as testemunhas se negarem a fornecer provas acerca dos sistemas que tinham utilizado.[39]

Intercepção secreta de sinais de grande capacidade

62. Sempre que o acesso a sinais de interesse não era possível por outras formas, as agências de Comint construíram equipamento de intercepção especial para instalar em embaixadas ou em outras instalações diplomáticas, ou até mesmo para transportar à mão para locais de interesse especial. Mike Frost, antigo funcionário da agência canadiana de Sigint, a CSE, publicou extensas descrições de operações deste género.[40] Embora as embaixadas nos centros das cidades estejam frequentemente localizadas de forma ideal para interceptar uma vasta gama de comunicações, desde serviços de telemóveis oficiais até ligações por microondas de grande capacidade, o processamento e a transmissão dessas informações pode ser difícil. Essas operações de recolha são também altamente sensíveis por questões diplomáticas. O equipamento para a recolha secreta é, consequentemente, especializado, selectivo e miniaturizado.

63. Um serviço de recolha especial conjunto da NSA e da CIA fabrica equipamento e forma o pessoal para actividades de recolha secreta. Um dos principais dispositivos é um sistema de processamento informático em formato de pasta, o ORATORY. Este sistema é, na realidade, uma versão miniaturizada dos computadores Dicionário descritos na secção seguinte, capaz de seleccionar comunicações não verbais de interesse a partir de uma gama alargada de fontes, de acordo com critérios de selecção previamente programados. Um dos principais fornecedores da NSA ("The IDEAS Operation") oferece agora receptores digitais micro-miniatura que podem

processar simultaneamente dados de Sigint de 8 canais independentes. Este receptor de rádio é do tamanho de um cartão de crédito. Enquadra-se num computador portátil normal. O fornecedor IDEAS afirma, sensatamente, que o seu minúsculo cartão executa funções que, ainda há pouco tempo, necessitariam de imenso equipamento.

Novas redes de satélites

64. Os operadores das novas redes construíram sistemas de telemóveis que facultam uma cobertura global ininterrupta utilizando satélites em órbitas terrestres baixas ou médias. Estes sistemas são, por vezes, denominados sistemas de comunicações pessoais via satélite (SPCS). Como cada satélite cobre apenas uma pequena área e se desloca rapidamente, são necessárias grandes quantidades de satélites para facultar uma cobertura global contínua. Os satélites podem transmitir os sinais directamente entre si ou para estações terrestres. O primeiro sistema deste género a ser terminado, o Iridium, utiliza 66 satélites e iniciou o seu funcionamento em 1998. O Iridium parece ter criado dificuldades consideráveis às agências de espionagem de comunicações, pois os sinais provenientes do Iridium e de redes semelhantes só podem ser recebidos numa pequena área, que pode ser em qualquer ponto da superfície da Terra.

3. ECHELON e produção de Comint

65. O sistema ECHELON tornou-se célebre após a publicação do relatório anterior do STOA. Desde então, novas provas mostram que o ECHELON já existia desde os anos 1970 e que foi grandemente ampliado entre 1975 e 1995. Tal como a intercepção de ILC, o ECHELON desenvolveu-se a partir de métodos anteriores. Esta secção inclui novas informações e provas documentais acerca do ECHELON e da intercepção de satélites.

A "lista de vigilância"

66. Depois da revelação pública do programa de intercepção SHAMROCK, o director da NSA, Tenente General Lew Allen, descreveu o modo como a NSA utilizava "listas de vigilância" como auxiliar na procura de actividades estrangeiras com interesse para as actividades de espionagem.[41] Afirmou que forneciam pormenores de mensagens contidas nas comunicações estrangeiras interceptadas que possuíssem nomes de indivíduos ou de organizações. Disse ainda que essas compilações de nomes eram vulgarmente referidas como "listas de vigilância".[42] Até à década de 1970, o processamento da lista de vigilância era manual. Os analistas examinavam as comunicações ILC interceptadas, reportando, fazendo "sínteses" ou analisando as que pareciam ocultar os nomes ou tópicos presentes na lista de vigilância.

Novas informações sobre unidades e sistemas do ECHELON

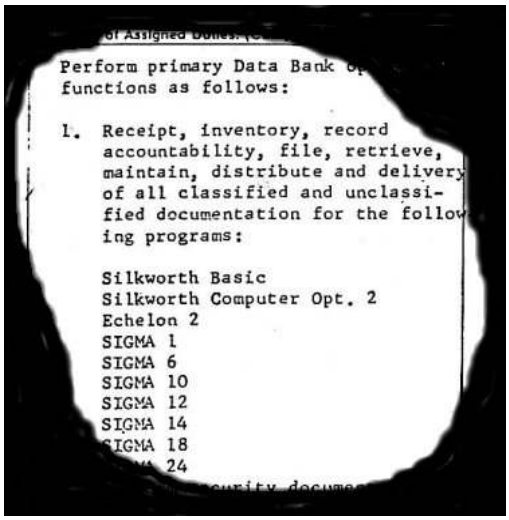
67. Parece agora que o sistema identificado como ECHELON já existia há mais de 20 anos. A necessidade de tal sistema foi prevista no final dos anos 1960, quando a NSA e o GCHQ planearam estações de intercepção de satélites de ILC em Mowenstow e Yakima. Esperava-se que a quantidade de mensagens interceptadas a partir dos

novos satélites fosse demasiado grande para ser examinada individualmente. Segundo o antigo pessoal da NSA, os primeiros computadores ECHELON automatizaram o processamento de Comint nestas unidades.[43]

68. A NSA e a CIA descobriram então que a recolha de Sigint a partir do espaço era mais eficaz do que tinham previsto, resultando em acumulações de gravações que excediam a quantidade existente de linguistas e analistas. Os documentos mostram que, quando os sistemas de processamento SILKWORTH foram instalados em Menwith Hill para os novos satélites, foram apoiados pelo ECHELON 2 e outros bancos de dados (consultar ilustração).

69. Em meados da década de 1980, as comunicações interceptadas nestas estações principais eram altamente esquadrinhadas, com uma grande variedade de especificações disponíveis para o tráfego não verbal. Foi planeada uma maior automatização em meados dos anos 80, sob o nome de Projecto P-415 da NSA. A implementação deste projecto completou a automatização da anterior actividade da lista de vigilância. A partir de 1987, o pessoal das agências internacionais de Comint viajou para os Estados Unidos, por forma a frequentar cursos de formação relativos aos novos sistemas informáticos.

70. O projecto P-415/ECHELON utilizou imenso a rede global de comunicações semelhante à Internet da NSA e do GCHQ para permitir que clientes de informação secreta remotos definissem tarefas para os computadores em cada unidade de recolha e que recebessem automaticamente os resultados. O principal componente do sistema são os computadores "Dicionário" locais, que armazenam uma grande base de dados sobre alvos específicos, incluindo nomes, tópicos de interesse, moradas, números de telefone e outros critérios de selecção. As mensagens recebidas são comparadas com esses critérios. Caso se encontre uma correspondência, a informação secreta não processada é reencaminhada automaticamente. Os computadores Dicionário são programados com milhares de requisitos de recolha diferentes, descritos como "números" (códigos de quatro dígitos).


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

A lista de bancos de dados de informação em Menwith Hill, em 1979, incluía a segunda geração do ECHELON

Unidade de intercepção de satélites ECHELON em Sugar Grove, Virgínia Ocidental, mostrando 6 antenas orientadas para satélites de comunicação europeus e do Atlântico (Novembro de 1998)

71. A definição de tarefas e a recepção de informação secreta dos computadores Dicionário envolve processos conhecidos por qualquer pessoa que já tenha utilizado a Internet. A triagem e selecção nestes computadores podem ser comparadas à utilização de motores de busca, que seleccionam páginas da Internet que contêm palavras ou termos-chave e especificam as relações. A função de reencaminhamento dos computadores Dicionário pode ser comparada ao correio electrónico. Quando solicitado, o sistema fornece listas de comunicações que correspondem a cada critério para que sejam revistas, analisadas, "sintetizadas" ou reencaminhadas. Um ponto importante acerca do novo sistema é que antes do ECHELON, países diferentes e estações diferentes sabiam o que estava a ser interceptado e a quem era enviado. Agora, praticamente quase todas as mensagens seleccionadas pelos computadores Dicionário, em unidades remotas, são reencaminhadas para a NSA ou para outros clientes sem serem lidas localmente.

Westminster, Londres - Computador Dicionário

72. Em 1991, um programa da televisão britânica noticiou as operações do computador Dicionário na delegação do GCHQ em Westminster, Londres. Segundo este programa, o sistema intercepta secretamente cada telex que entre, saia ou passe por Londres; milhares de mensagens diplomáticas, comerciais e pessoais todos os dias. Estas são inseridas num programa conhecido como "Dicionário" que escolhe palavras-chave no conjunto de Sigint e persegue centenas de indivíduos e corporações.[44] O programa salientava que os computadores Dicionário, embora controlados e programados pelo GCHQ, eram operados por pessoal de segurança empregados pela British Telecom (BT), o principal operador de telecomunicações em Inglaterra.[45] A presença de computadores Dicionário foi também confirmada em Kojarena, Austrália, e no GCHQ de Cheltenham, Inglaterra.[46]

Sugar Grove, Virgínia - Intercepção de COMSAT na unidade ECHELON

73. Documentos do governo dos Estados Unidos confirmam que a estação de recepção de satélite em Sugar Grove, na Virgínia Ocidental, é uma unidade ECHELON e que recolhe informação secreta de COMSAT. A estação encontra-se a cerca de 400 km a sudoeste de Washington, numa área remota das Montanhas Shenandoah. É operada pelo Naval Security Group e pela Air force Intelligence Agency dos Estados Unidos.

74. Um sistema actualizado, chamado TIMBERLINE II, foi instalado em Sugar Grove, no Verão de 1990. Na mesma altura, segundo documentos oficiais norte-americanos, foi estabelecido um departamento de formação em ECHELON.[47] Tendo finalizado a formação, a tarefa da estação, em 1991, passou a ser **a manutenção e o funcionamento de uma unidade ECHELON**.[48]

75. A Força Aérea dos Estados Unidos identificou publicamente a actividade de informação em Sugar Grove, declarando que a sua missão era a de **orientar o equipamento de comunicações via satélite para auxiliar consumidores de informações COMSAT**. Isto é feito através de um quadro de gestores, analistas e operadores formados em sistemas de recolha.[49] Em 1990, fotografias por satélite mostraram que existiam 4 antenas de satélite em Sugar Grove. Em Novembro de 1998, uma inspecção no terreno revelou que se tinha expandido para um grupo de 9.

Sabana Seca, Porto Rico e Leitrim, Canadá - Unidades de intercepção de COMSAT

76. Informações adicionais publicadas pela Força Aérea dos Estados Unidos identificam a estação do Naval Security Group dos Estados Unidos em Sabana Seca, Porto Rico, como uma unidade de intercepção de COMSAT. A sua missão é a de se tornar a primeira estação de campo para o **processamento e a análise de comunicações via satélite**.[50]

77. As Forças de Defesa canadianas publicaram pormenores sobre as funções do respectivo pessoal na estação de campo de Leitrim da agência de Sigint canadiana CSE. A estação, perto de Ottawa, Ontário, tem quatro terminais de satélite, erigidos desde 1984. Entre o pessoal encontram-se sete analistas de satélites de comunicações, supervisores e instrutores.[51]

78. Num currículo disponível para o público em geral, um antigo analista de satélites de comunicações, que trabalhava em Leitrim, descreve o seu trabalho como tendo a experiência necessária em termos de **operação e análise de numerosos sistemas informáticos de Comsat e dos subsistemas relacionados, utilizando sistemas de análise assistidos por computador e uma vasta gama de equipamento electrónico sofisticado para interceptar e estudar comunicações estrangeiras e transmissões electrónicas**.[52] Relatórios financeiros da CSE indicam também que, em 1995/96, a agência planeava pagamentos de 7 milhões de dólares para o ECHELON e de 6 milhões de dólares para os computadores Cray. Não existiam mais pormenores sobre o ECHELON.[53]

Waihopai, Nova Zelândia - Intercepção da Intelsat na unidade ECHELON

79. A agência de Sigint neozelandesa GCSB opera dois terminais de intercepção de satélites em Waihopai, direccionados para satélites Intelsat que cobrem o Oceano Pacífico. Já foram publicados pormenores consideráveis sobre os computadores Dicionário da estação e o respectivo papel na rede ECHELON.[54] Depois de o livro ter sido publicado, uma estação televisiva neozelandesa obteve imagens do interior do centro de operações da estação. As imagens foram obtidas clandestinamente, filmadas durante a noite, através de janelas com cortinas entreabertas. O repórter da televisão conseguiu filmar grandes planos de manuais técnicos no centro de controlo. Tratava-se de **manuais técnicos de Intelsat**, confirmando que a estação tinha este tipo de satélites como alvos. Para grande surpresa, a estação parecia estar praticamente vazia, a trabalhar totalmente de forma automática. Havia um guarda no interior, mas não se apercebeu de que estava a ser filmado.[55]

Técnicas de processamento ILC

80. O anexo técnico descreve os principais sistemas utilizados para extrair e processar informações secretas obtidas nas comunicações. As explicações pormenorizadas dadas acerca dos métodos de processamento não são essenciais para a compreensão da essência deste relatório, mas são fornecidas para que os leitores com conhecimentos sobre telecomunicações possam avaliar completamente a tecnologia de ponta.

81. As mensagens por fax e os dados informáticos (de *modems*) têm prioridade no processamento devido à facilidade com que são compreendidas e analisadas. O principal método de filtragem e de análise de tráfego não verbal, os computadores Dicionário, utilizam técnicas tradicionais de recuperação de informações, incluindo palavras-chave. *Chips* especiais rápidos permitem que grandes quantidades de dados sejam processadas desta forma. A técnica mais recente é a "detecção de tópicos". O processamento de chamadas telefónicas está principalmente limitado à identificação de informações relacionadas com a chamada e à análise do tráfego. Não existem sistemas eficazes de "detecção de palavras", apesar dos relatos em contrário. Mas, pelo menos desde 1995, têm sido utilizados sistemas de identificação do orador do tipo "perfil vocal". A utilização de criptografia consistente está lentamente a colidir com as capacidades das agências de Comint. Esta dificuldade para as agências de Comint tem sido contrabalançada por actividades secretas e abertas que subverteram a eficácia dos sistemas criptográficos fornecidos e/ou utilizados na Europa.

82. As conclusões tiradas no anexo indicam que o equipamento de Comint actualmente disponível tem a possibilidade, conforme for programado, de interceptar, processar e analisar todos os tipos modernos de sistemas de comunicações de grande capacidade a que se consiga obter acesso, incluindo os níveis mais elevados da Internet. Existem algumas falhas na cobertura. A escala, a capacidade e a velocidade de alguns sistemas são difíceis de compreender na totalidade. Foram construídos sistemas especiais para processar mensagens de *pagers*, rádios móveis celulares e novos satélites.

4. Comint e a aplicação da lei

83. Em 1990 e 1991, o Governo norte-americano começou a preocupar-se com o facto de a comercialização de um sistema telefónico seguro pela AT&T poder prejudicar a actividade de Comint. A AT&T foi persuadida a retirar o produto do mercado. Em substituição, o Governo norte-americano ofereceu à NSA *chips* "Clipper" para incorporação em telefones seguros. Os *chips* seriam fabricados pela NSA, que gravaria também chaves incorporadas e que transmitiria estas informações a outras agências governamentais para armazenamento e, se necessário, recuperação. Esta proposta provou ser extremamente impopular e foi abandonada. Em sua substituição, o Governo norte-americano propôs que as agências não governamentais devessem manter cópias de cada chave de utilizador, num sistema denominado de "depósito da chave" e, posteriormente, de "recuperação de chave". Em retrospectiva, a verdadeira finalidade destas propostas era a de fornecer à NSA um ponto único (ou poucos pontos) de acesso às chaves, o que lhes permitiria continuar a ter acesso a comunicações privadas e comerciais.

Deturpação das necessidades de intercepção para aplicação da lei

84. Entre 1993 e 1998, os Estados Unidos realizaram actividades diplomáticas sustentadas, tentando persuadir as nações da UE e a OCDE a adoptar o seu sistema de "recuperação de chave". Ao longo deste período, o Governo norte-americano insistiu em que a finalidade desta iniciativa era a de auxiliar as entidades responsáveis pela aplicação da lei. Os documentos obtidos para este estudo sugerem que estas afirmações deturpavam, intencionalmente, a verdadeira intenção da política norte-

americana. Documentos obtidos ao abrigo da lei da liberdade de informação norte-americana indicam que a elaboração de políticas era liderada exclusivamente por funcionários da NSA, por vezes excluindo totalmente agentes da polícia ou funcionários judiciais. Por exemplo, quando o "Embaixador da Criptografia", David Aaron, que havia sido especialmente nomeado, visitou a Inglaterra em 25 de Novembro de 1996, ia acompanhado e instruído pelo principal representante da NSA em Inglaterra, o Dr. James J. Hearn, antigo subdirector da NSA. David Aaron não consultou nem se encontrou com funcionários do FBI adidos da sua embaixada. A sua reunião com funcionários do Governo britânico incluiu o representante da NSA e pessoal do GCHQ britânico, mas excluiu agentes da polícia e funcionários judiciais de ambas as nações.

85. Desde 1993, sem o conhecimento dos organismos parlamentares europeus e dos respectivos eleitores, os agentes de aplicação da lei de muitos países da UE e a maioria das nações da UKUSA têm tido encontros anuais, num fórum separado, para discutir os seus requisitos em termos de intercepção de comunicações. Estes agentes encontraram-se sob a égide de uma organização até aqui desconhecida, o ILETS (Seminário Internacional sobre a Vigilância Legal das Telecomunicações). O ILETS foi iniciado e fundado pelo FBI. O quadro 2 apresenta uma lista das reuniões do ILETS realizadas entre 1993 e 1997.

86. Nas reuniões de 1993 e 1994, os participantes do ILETS especificaram requisitos do utilizador para a aplicação da lei relativamente à intercepção de comunicações. Estes aparecem num documento do ILETS de 1974 denominado "IUR 1.0". Este documento baseava-se num relatório anterior do FBI relativo aos “requisitos de aplicação da lei para a vigilância de comunicações electrónicas”, emitido pela primeira vez em Julho de 1992 e revisto em Junho de 1994. Os requisitos do IUR pouco diferiam em substância dos requisitos do FBI, mas foram alargados, contendo dez requisitos em vez de nove. **O IUR não especificava <u>qualquer</u> necessidade de aplicação da lei para o "depósito da chave" ou para a "recuperação das chaves"**. A criptografia era mencionada apenas no contexto das disposições de segurança da rede.

87. Entre 1993 e 1997, os representantes da polícia do ILETS não foram envolvidos no processo de elaboração de políticas liderado pela NSA relativamente à "recuperação da chave", nem o ILETS apresentou qualquer proposta deste género, nem sequer em 1997. Apesar deste facto, durante o mesmo período, o Governo norte-americano apresentou repetidamente a sua política como estando motivado pelas necessidades indicadas pelas entidades responsáveis pela aplicação da lei. Na reunião de 1997 em Dublin, o ILETS não alterou o IUR. Só em 1998 viria a ser preparado um IUR revisto contendo os requisitos referentes a criptografia. Consequentemente, o Governo norte-americano induziu os Estados da UE e da OCDE em erro relativamente à verdadeira intenção desta política.

88. Contudo, este engano por parte dos norte-americanos era claro para o alto-funcionário da Comissão responsável pela segurança das informações. Em Setembro de 1996, David Herson, chefe do grupo de altos-funcionários para a segurança da informação da UE, fez a sua avaliação do projecto norte-americano de "recuperação da chave". De acordo com este funcionário, a "aplicação da lei" é um escudo de protecção para todas as outras actividades governamentais. Tratava-se de informação secreta estrangeira e não havia qualquer dúvida que a "aplicação da lei" era apenas uma cortina de fumo.[56]

89. Dever-se-á notar que, do ponto de vista técnico, legal e organizacional, os requisitos de aplicação da lei para a intercepção de comunicações diferem fundamentalmente da espionagem de comunicações. As entidades responsáveis pela aplicação da lei normalmente desejam interceptar uma linha ou um grupo de linhas específicos e, geralmente, têm de justificar os seus pedidos a uma autoridade judicial ou administrativa antes de prosseguirem. Por contrato, as agências de Comint levam a cabo vastas actividades "por arrasto" em comunicações internacionais e operam ao abrigo de mandatos gerais. Essas operações não requerem, nem sequer pressupõem, que as partes interceptadas sejam criminosos. Essas distinções são vitais para a liberdade civil, mas ficarão em risco se os limites entre a intercepção para aplicação da lei e a intercepção para obter espionagem de comunicações se tornarem indistintos no futuro.

Ano	*Local*	*Participantes de países terceiros*	*Participantes da UE*
1993	Quantico, Virginia, EUA	Austrália, Canadá, Hong Kong, Noruega, Estados Unidos	Dinamarca, França, Alemanha, Países Baixos, Espanha, Suécia, Reino Unido
1994	Bona, Alemanha	Austrália, Canadá, Hong Kong, Noruega, Estados Unidos	Áustria, Bélgica, Dinamarca, Finlândia, França, Alemanha, Grécia, Irlanda, Luxemburgo, Países Baixos, Portugal, Espanha, Suécia, Reino Unido
1995	Camberra, Austrália	Austrália, Canadá, Hong Kong, Nova Zelândia, Noruega, Estados Unidos	Bélgica, França, Alemanha, Grécia, Irlanda, Itália, Países Baixos, Espanha, Suécia, Reino Unido
1997	Dublim Irlanda	Austrália, Canadá, Hong Kong, Nova Zelândia, Noruega, Estados Unidos	Áustria, Bélgica, Dinamarca, Finlândia, França, Alemanha, Irlanda, Itália, Luxemburgo, Países Baixos, Portugal, Espanha, Suécia, Reino Unido

Quadro 2: Reuniões do ILETS, 1993-1997

Intercepção de comunicações para aplicação da lei - desenvolvimento de políticas na Europa

90. A seguir à segunda reunião do ILETS, em Bona, em 1994, o IUR 1.0 foi apresentado ao Conselho de Ministros e foi aprovado, sem que se alterasse uma só palavra, a 17 de Janeiro de 1995.[57] Em 1995, vários membros do ILETS não pertencentes à UE escreveram ao Conselho para adoptar a resolução do mesmo (por publicar). A resolução só foi publicada no Jornal Oficial quase dois anos depois, a 4 de Novembro de 1996.

91. No seguimento da terceira reunião do ILETS em Camberra, em 1995, foi solicitado ao Governo australiano que apresentasse o IUR à União Internacional das Telecomunicações (UIT). Notando que as entidades responsáveis pela aplicação da lei e pela segurança nacional de um número significativo de países membros da UIT acordaram num conjunto genérico de requisitos para a intercepção legal, o Governo australiano pediu à UIT que aconselhasse os seus órgãos a incorporar os requisitos do IUR em futuros sistemas de telecomunicações, com base no facto de ser possível reduzir os custos do fornecimento de uma capacidade de intercepção legal e perturbações associadas, se esta capacidade for fornecida na fase da concepção.[58]

92. Parece que o ILETS se reuniu novamente em 1998 e reviu e alargou as suas disposições, por forma a abranger a Internet e os sistemas de comunicações pessoais via satélite, como o Iridium. O novo IUR especificava também requisitos de segurança adicionais para os operadores de rede e para os fornecedores de serviços, novos

requisitos extensivos para as informações pessoais sobre assinantes e disposições relativas à criptografia.

93. A 3 de Setembro de 1998, o IUR revisto foi apresentado ao Grupo de Trabalho de Cooperação Policial como ENFOPOL 98. A Presidência austríaca propôs que, tal como em 1994, o novo IUR fosse adoptado integralmente como Resolução do Conselho relativa à intercepção de novas tecnologias.[59] O grupo não concordou. Após repetidas reformulações, foi preparado um documento novo pela Presidência alemã, para a eventual consideração por parte dos ministros do Interior e da Justiça do Conselho.[60]

5. Comint e espionagem económica

94. Durante o debate do PE, em 1998, sobre as relações transatlânticas e o sistema ECHELON, o Comissário Bangeman observou, em nome da Comissão, que se esse sistema existisse, seria um ataque intolerável contra as liberdades individuais, a concorrência e a segurança dos Estados.[61] A existência do ECHELON foi descrita na secção 3 acima. Esta secção descreve as estruturas de organização e de relato nas quais as informações sensíveis do ponto de vista económico recolhidas pelo ECHELON e por sistemas relacionados são divulgadas, resumindo exemplos em que organizações europeias foram alvo de vigilância.

Missões de espionagem económica

95. Funcionários norte-americanos reconhecem que a NSA recolhe informações económicas, intencionalmente ou não. O antigo adido militar, Coronel Dan Smith, trabalhou na embaixada dos Estados Unidos em Londres até 1993. Recebia regularmente produtos Comint provenientes de Menwith Hill. Em 1998, ele disse à BBC que em Menwith Hill, em termos de recolha de comunicações, como trabalhavam em banda larga, inevitavelmente haveria conversas ou comunicações que eram interceptadas, sem estarem minimamente relacionadas com a área militar. Entre elas, provavelmente existiriam algumas informações sobre assuntos comerciais. Disse também que, tecnicamente, tudo seria possível. Poderiam recolher todas estas informações, separá-las e descobrir o que poderia ser necessário, embora não existisse qualquer política para o fazer especificamente em resposta ao interesse de uma determinada empresa.[62]

96. Em geral, esta afirmação não está incorrecta, mas ignora distinções fundamentais entre a recolha e a divulgação e entre espionagem comercial e económica. Não existem quaisquer provas de que empresas em qualquer um dos países da UKUSA sejam capazes de efectuar a recolha de Comint por forma a satisfazer as suas finalidades individuais. Nem têm de o fazer. Cada país da UKUSA autoriza organizações nacionais de avaliação de informações secretas e os ministérios relevantes a solicitar e receber informações económicas secretas do Comint. Essas informações podem ser recolhidas para imensas finalidades, tais como: calcular os futuros preços de bens essenciais; determinar as posições de outras nações em negociações comerciais; controlar o comércio internacional de armas; detectar tecnologias sensíveis; ou avaliar a estabilidade política e/ou a força económica de um

determinado país. Qualquer destes alvos, e muitos outros, podem produzir informações de relevância comercial directa. A decisão de divulgar ou explorar estas informações não é tomada por agências de Comint, mas sim por organizações governamentais nacionais.

Divulgação de informação económica secreta

97. Em 1970, de acordo com o ex-director executivo do Foreign Intelligence Advisory Board dos Estados Unidos, este serviço recomendou que, daí em diante, a espionagem económica devia ser considerada uma função da segurança nacional, gozando de uma prioridade equivalente à da informação diplomática, militar ou tecnológica.[63] A 5 de Maio de 1977 uma reunião entre a NSA, a CIA e o Departamento de Comércio autorizou a criação de um novo departamento secreto, o "Office of Intelligence Liaison". A sua tarefa era lidar com "informação secreta estrangeira" de interesse para o Departamento de Comércio. O regulamento deste novo departamento mostra que estava autorizado a receber e a tratar informações secretas SCI - Comint e Sigint da NSA. A criação deste departamento constituiu assim um mecanismo formal onde os dados da NSA podiam ser utilizados para apoiar interesses comerciais e económicos. Depois deste sistema ser realçado num programa da televisão britânica em 1993, o seu nome foi mudado para (Office of Executive Support).[64] Também em 1993, o Presidente Clinton alargou o apoio norte-americano em termos de espionagem a organizações comerciais criando um novo National Economic Council (Conselho Económico Nacional), paralelo ao Conselho Nacional de Segurança.

98. A natureza deste apoio foi largamente divulgada. Antigos funcionários do serviço de espionagem e outros especialistas indicavam que as sugestões com base na espionagem frequentemente saíam do Departamento de Comércio para empresas norte-americanas, para as ajudar a ganhar contratos no estrangeiro.[65] O Gabinete de Apoio Executivo fornece informações secretas semanais a agentes de segurança. Um jornal norte-americano obteve relatórios do Departamento de Comércio que demonstram o apoio, em termos de informação secreta, prestado a empresas norte-americanas. Segundo esse jornal, um desses documentos é a acta de uma reunião do Departamento de Comércio, realizada em Agosto de 1994, com vista à identificação dos principais contratos a concurso na Indonésia, para que as empresas norte-americanas ganhassem a empreitada. Um funcionário da CIA falou durante a reunião. Cinco das 16 pessoas na lista de distribuição da acta pertenciam à CIA.

99. No Reino Unido, o GCHQ é obrigado por lei (e conforme e sempre que for solicitado pelo Governo britânico) a interceptar comunicações estrangeiras, no interesse do bem-estar económico do Reino Unido, relativamente às acções ou intenções de pessoas fora das Ilhas Britânicas. A intercepção comercial é solicitada e analisada pela Divisão K do GCHQ. Os alvos comerciais e económicos podem ser especificados pela Overseas Economic Intelligence Committee do governo, pelo pessoal do Joint Intelligence Committee (JIC), pelo Tesouro ou pelo Banco de Inglaterra.[66] De acordo com um antigo alto-funcionário da JIC, a actividade de Comint normalmente inclui planos de empresas, telexes, faxes e chamadas telefónicas transcritas. Muitas destas eram chamadas entre a Europa e o Hemisfério Sul.[67]

100. Na Austrália, a Comint que seja comercialmente relevante é enviada pelo DSD para o Office of National Assesments, que considera se, e nesse caso onde, se deve divulgar a Comint. O pessoal deste departamento pode passar as informações para

empresas australianas se acreditar que uma nação estrangeira tem ou procura ter uma vantagem comercial desleal. Os alvos desta actividade incluíram a Thomson-CSF e as negociações comerciais com compradores japoneses de carvão e minério de ferro. Os outros países da UKUSA, o Canadá e a Nova Zelândia, possuem sistemas semelhantes em funcionamento.

Utilização do produto de espionagem económica Comint

Consórcio Panavia para a construção do Avião de Combate Europeu Aéreos Panavia e Arábia Saudita

101. Em 1993, num programa acerca de Menwith Hill, Howard Teicher, antigo funcionário do Conselho Nacional de Segurança, descreveu como a empresa europeia Panavia estava especificamente orientada para as vendas no Médio Oriente. Afirmou que se lembrava que as palavras "Tornado" ou "Panavia" - informações relacionadas com esta aeronave específica - seriam alvos prioritários sobre os quais gostariam de obter informações.[68]

Thomson-CSF e Brasil

102. Em 1994, a NSA interceptou telefonemas entre a Thomson-CSF e o Brasil, relativos ao SIVAM, um sistema de vigilância para a floresta tropical da Amazónia, no valor de 1,3 mil milhões de dólares. Alegava-se que a empresa tinha subornado membros do painel de selecção do Governo brasileiro. O contrato foi adjudicado à empresa norte-americana Raytheon Corporation, que anunciou posteriormente que o Departamento do Comércio tinha trabalhado muito para apoiar a indústria norte-americana nesse projecto.[69] A empresa Raytheon fornece também serviços de manutenção e de engenharia à estação de intercepção de satélites ECHELON da NSA, em Sugar Grove.

Airbus Industrie e Arábia Saudita

103. Segundo um relato na imprensa, documentado, de 1995, a NSA, a partir de um satélite de comunicações comerciais, recolhia todos os faxes e telefonemas entre o consórcio europeu Airbus, a transportadora aérea nacional da Arábia Saudita e o Governo deste país. A agência descobriu que os agentes da Airbus ofereciam subornos a um funcionário saudita. Transmitiu as informações a funcionários norte-americanos que lidavam com a proposta da Boeing Co. e da McDonnell Douglas Corp., que triunfaram neste concurso, em 1994, no valor de 6 mil milhões de dólares.[70]

Negociações comerciais internacionais

104. Foram publicados muitos outros relatos por jornalistas com grande reputação e vários testemunhos em primeira mão citavam ocasiões frequentes em que o governo dos Estados Unidos tinha utilizado a Comint para finalidades comerciais nacionais. Estas incluem a procura de dados sobre as normas de emissão dos veículos japoneses,[71] as negociações de 1995 relativas à importação de automóveis de luxo japoneses,[72] a participação francesa nas negociações do GATT em 1993 e a Conferência Económica Ásia-Pacífico (APEC) em 1997.

Vigilância das nações anfitriãs

105. Levanta-se também a questão da possibilidade de os Estados Unidos utilizarem unidades de espionagem de comunicações, como a de Menwith Hill ou a de Bad Aibling, para atacar as comunicações das nações anfitriãs. As provas disponíveis sugerem que essa conduta pode normalmente ser evitada. Segundo o antigo funcionário do Conselho Nacional de Segurança, Howard Teicher, o Governo norte-americano não instruiria a NSA para espiar um governo anfitrião como a Inglaterra, embora afirme que nunca diria nunca nesta área, já que, afinal, os interesses nacionais são interesses nacionais e, por vezes, os interesses das nações divergem, especialmente nesta área.

6. Capacidade de Comint após o ano 2000

Desenvolvimento tecnológico

106. Desde meados da década de 90, as agências de espionagem de comunicações têm enfrentado dificuldades substanciais em manter o **acesso** global aos sistemas de comunicações. Estas dificuldades aumentarão durante e após o ano 2000. A principal razão para isto é a mudança das telecomunicações para redes de fibra óptica de grande capacidade. Para a intercepção, é necessário o acesso físico aos cabos. A não ser que a rede de fibra esteja ou passe por um Estado colaborador, a intercepção eficaz é feita praticamente apenas pela adulteração com repetidores opto-electrónicos (se instalados). Esta limitação irá, provavelmente, colocar fora de alcance muitas redes de fibra óptica de grande capacidade sediadas em terreno estrangeiro. As dimensões físicas do equipamento necessário para processar o tráfego, juntamente com os sistemas de energia, comunicações e gravação, tornam a actividade clandestina difícil de praticar e arriscada.

107. Mesmo quando o acesso fica facilmente disponível (como para os COMSAT), a proliferação de novos sistemas limitará as actividades de **recolha**, em parte porque as limitações orçamentais diminuirão o número de novas instalações e em parte porque não se consegue ter acesso a alguns sistemas (por exemplo, o Iridium) através dos sistemas actualmente disponíveis.

108. Nos últimos 15 anos, a liderança tecnológica substancial em termos de tecnologia informática e da informação, de que gozavam outrora as organizações Comint, praticamente desapareceu. Os seus principais sistemas informáticos são comprados em lojas e são iguais ou mesmo inferiores aos utilizados pelas organizações industriais e académicas de primeira linha. A única diferença é o facto de serem "blindados contra TEMPEST", o que evita que emitam sinais de rádio que podiam ser utilizados para analisar a actividade de Sigint.

109. As organizações de espionagem de comunicações reconhecem que a demorada guerra contra a criptografia civil e comercial foi perdida. Uma comunidade académica e

industrial próspera tem grandes capacidades em termos de criptografia e criptologia. A Internet e o mercado global criaram um fluxo livre de informações, sistemas e software. A NSA fracassou na sua missão de perpetuar o acesso a estes sistemas ao fingir que o "depósito da chave" e sistemas semelhantes se destinavam a apoiar os requisitos de aplicação da lei (ao contrário da Comint).

110. As tendências futuras para a Comint incluirão, provavelmente, limites ao investimento em recolha de Comint a partir do espaço, uma maior utilização de agentes humanos para a colocação de dispositivos de recolha ou para a obtenção de códigos do que no passado, e um esforço reforçado para atacar sistemas informáticos estrangeiros, utilizando a Internet e outros meios (em especial, para obter acesso a ficheiros protegidos ou a comunicações antes de serem criptografados).

111. As tentativas de limitar a criptografia conseguiram, mesmo assim, atrasar a introdução em grande escala de sistemas de segurança criptográficos eficazes. Os custos reduzidos do poder informático permitiram também que as agências de Comint criassem ferramentas de processamento e de classificação rápidas e sofisticadas.

112. Recentes comentários feitos a veteranos da CIA pelo chefe da House of Representatives Permanent Select Committee on Intelligence dos Estados Unidos, o ex-funcionário da CIA John Millis, ilustram a forma como a NSA encara as mesmas questões. Segundo ele, a informação sobre sinais está em crise, tendo no passado a tecnologia sido aliada da NSA mas, nos últimos quatro ou cinco anos, deixado de ser aliada da Sigint para se tornar sua inimiga. John Millis acrescentou ainda que os meios de comunicação tinham deixado de ser compatíveis com a Sigint e que, ao serem emitidos sinais de RF, qualquer pessoa no alcance desses sinais poderia recebê-los tão nitidamente quanto o destinatário pretendido. Millis acrescentou que a tecnologia deixara de ser essa para passar a ser de microondas e que as pessoas tinham descoberto uma óptima maneira de também a aproveitar. Afirmou ainda que actualmente avançamos para meios aos quais é difícil ter acesso; a criptografação existe e irá evoluir muito rapidamente, o que é mau para a Sigint, pois vai ser necessário investir muito dinheiro em novas tecnologias para se obter acesso e para se conseguir decifrar as informações que ainda necessitamos de obter da Sigint.

Questões políticas para o Parlamento Europeu

1. A resolução parlamentar de 1998 relativa às relações transatlânticas e ao sistema ECHELON[73] apelava a medidas de protecção no que diz respeito à informação económica e a uma criptografação eficaz. O fornecimento dessas medidas pode ser facilitado pelo desenvolvimento de uma compreensão aprofundada sobre as capacidades actuais e futuras da Comint.

2. Ao nível técnico, as medidas de protecção podem ser concentradas para derrotar a actividade de Comint hostil, negando o acesso ou, onde isto for impraticável ou impossível, evitando o processamento dos conteúdos de mensagens e das informações de tráfego associadas através da utilização geral da criptografia.

3. Tal como reconheceu o grupo SOGIS (Grupo de altos Funcionários para a Segurança da Informação) no seio da Comissão,[74] os interesses divergentes entre Estados são uma questão complexa. Os Estados de maiores dimensões fizeram investimentos substanciais em capacidades de Comint. Um Estado-Membro está activo na aliança UKUSA, enquanto outros são "terceiros contratantes" da UKUSA ou fizeram acordos bilaterais com a NSA. Alguns destes acordos foram legados da "guerra fria", outros ainda duram. Estas questões criam conflitos de interesses internos e internacionais. As soluções técnicas não são óbvias. Deveria ser possível definir um interesse partilhado na implementação de medidas para derrotar futuras actividades de Comint externas dirigidas contra Estados europeus, seus cidadãos e actividades comerciais.

4. Uma segunda área de aparente conflito diz respeito ao desejo por parte dos Estados de facultar a intercepção de comunicações com fins legítimos de aplicação da lei. Os processos técnicos e legais envolvidos na provisão de intercepção com fins de aplicação da lei diferem fundamentalmente daqueles utilizados na espionagem de comunicações. Em parte devido à falta de consciência parlamentar e pública relativamente às actividades de Comint, esta distinção é frequentemente encoberta, especialmente pelos Estados que investem fortemente em Comint. Qualquer fracasso na distinção entre requisitos legítimos da intercepção para aplicação da lei e a intercepção para fins de espionagem levanta graves questões relativamente às liberdades civis. Uma fronteira clara entre a actividade de intercepção para aplicação da lei e por motivos de "segurança nacional" é essencial para a protecção dos direitos humanos e das liberdades fundamentais.

5. Actualmente, os *browsers* da Internet e outro *software* utilizado em quase todos os computadores pessoais existentes na Europa são deliberadamente desactivados para que as comunicações "seguras" que enviam possam, caso sejam recolhidas, ser lidas sem dificuldade pela NSA. Os fabricantes norte-americanos são forçados a tomar estas providências ao abrigo das leis de exportação norte-americanas. É importante existir um campo de acção nivelado. Deverá considerar-se uma contramedida através da qual os sistemas com dispositivos criptográficos desactivados, caso sejam vendidos fora dos Estados Unidos, estejam em conformidade com uma "norma aberta" que permita que terceiros e outras nações possam facultar aplicações adicionais que reponham o nível de segurança, no mínimo, no nível gozado pelos clientes norte-americanos.

6. O trabalho do ILETS prosseguiu durante 6 anos sem o envolvimento de parlamentares e sem consultar as organizações industriais, cujos interesses fundamentais são afectados pelo trabalho deste organismo. É de lamentar que, antes da publicação deste relatório, não existisse qualquer tipo de informação pública nos Estados acerca do âmbito dos processos de elaboração de políticas, dentro e fora da UE, que levaram à formulação de "requisitos do utilizador" existentes e novos para a aplicação da lei. Como questão urgente, o processo actual de elaboração de políticas deveria ser aberto ao público e à discussão parlamentar nos Estados-Membros e no PE, para que se possa encontrar um equilíbrio adequado entre os direitos de segurança e privacidade dos cidadãos e das empresas, os interesses financeiros e técnicos dos operadores de redes e fornecedores de serviços de comunicações, e a necessidade de apoiar as actividades de aplicação da lei que se destinam a suprimir o crime e o terrorismo grave.

Anexo técnico

Comunicações de banda larga (multi-canal de grande capacidade)

1. Desde 1950 até ao início da década de 1980, os sistemas de comunicações analógicos multi-canal de grande capacidade foram normalmente concebidos utilizando diferentes canais de comunicação transportados em frequências diferentes. O sinal combinado, que poderia incluir 2.000 canais de voz ou mais, era um "multiplex". O sinal de "multiplex por divisão de frequência" (FDM) resultante era então transportado numa frequência muito mais elevada, como um sinal de rádio por microondas.

2. As comunicações digitais já quase substituíram universalmente os métodos analógicos. O sistema básico de comunicações digitais multi-canal é o multiplex por divisão de tempo (TDM). Num sistema de telefonia TDM, os canais individuais de conversação são, em primeiro lugar, digitados. As informações relativas a cada canal são depois transmitidas sequencialmente, em vez de simultaneamente, ocupando cada ligação "intervalos" de tempo sucessivos.

3. As normas relativas às comunicações digitais evoluíram de forma independente na Europa e na América do Norte. Nos Estados Unidos, o sistema de telecomunicações público então dominante (o sistema Bell, gerido pela AT&T) estabeleceu normas para os dados digitais. O bloco de construção básico, a ligação T-1, transporta o equivalente a 24 canais telefónicos a uma velocidade de 1,544 Mbps. Os sistemas de maior capacidade trabalham a velocidades de transmissão de dados superiores. Consequentemente, a velocidade de transmissão mais elevada, a da ligação T-5, transporta o equivalente a 8.000 canais de voz a uma velocidade de 560 Mbps.

4. A Europa adoptou uma estrutura diferente para comunicações digitais, com base nas normas inicialmente acordadas pelo CECT. A ligação digital básica na Europa, a E-1, transporta 30 canais telefónicos a uma velocidade de dados de 2 Mbps. A maior parte dos sistemas de telecomunicações europeus baseia-se em ligações E-1 ou (como na América do Norte) em múltiplos desta. A distinção é significativa porque a maioria do equipamento de processamento de Comint fabricado nos Estados Unidos está concebido para lidar com comunicações interceptadas que trabalhem segundo as formas europeias de comunicação digital.

5. Os sistemas digitais recentes utilizam sinais sincronizados transportados por fibras ópticas de enorme capacidade. A sincronização dos sinais permite que canais individuais sejam facilmente extraídos de ligações de alta capacidade. O novo sistema é conhecido nos Estados Unidos como rede óptica síncrona (SONET), embora sejam utilizadas três definições e rótulos equivalentes.[75]

Equipamento de espionagem de comunicações

6. Dezenas de fornecedores norte-americanos no campo da defesa, muitos dos quais situados em Silicon Valley (Califórnia) ou na área da "cintura" de Maryland, perto de Washington, fabricam equipamento de Sigint sofisticado para a NSA. Grandes

corporações norte-americanas, como a Lockheed Martin, a Space Systems/Loral, a TRW, a Raytheon e a Bendix, são também contratadas pela NSA para gerir as principais unidades de recolha de Sigint. Este estudo não tem por objectivo elaborar um relatório completo dos produtos e serviços destas empresas. A tecnologia de ponta de espionagem de comunicações contemporâneas poderá ser utilmente demonstrada, contudo, através do exame de alguns dos produtos de processamento de Comint de dois dos fornecedores especializados da NSA: a Applied Signal Techcnology Inc. (AST) de Sunnyvale, Califórnia e a The IDEAS Operation de Columbia, Maryland (parte da Science Applications International Corporation (SAIC)).[76]

7. Ambas as empresas têm ex-funcionários superiores da NSA como directores. Quando não estiver explicitamente indicado, os produtos destas empresas podem ser identificados como destinados para Sigint por terem sido "testados contra TEMPEST". A AST declara geralmente que o seu equipamento é utilizado para o reconhecimento de sinais de comunicações estrangeiras por parte do governo dos Estados Unidos. Um importante criptógrafo descreveu apta e insinuantemente a AST como uma "loja" de ECHELON onde se pode comprar tudo.

Extracção de banda larga e análise de sinais

8. Os sinais de banda larga são normalmente interceptados a partir de satélites ou cabos submetidos a escutas, sob a forma de microondas multiplex ou de sinais de alta frequência. O primeiro passo para o processamento desses sinais para fins de Comint consiste na "**extracção de banda larga**". Uma vasta gama de equipamento de Sigint é fabricada com este fim, permitindo a vigilância e a análise de sistemas recentemente interceptados. Entre estes encontra-se o equipamento de estudos de transmissores-receptores que identificam e classificam ligações descendentes de satélites, desmoduladores, descodificadores, desmultiplexadores, sistemas de análise de ligações por rádio de microondas, unidades de estudo de ligações, sistemas de análises de portadoras e muitas outras formas de *hardware* e de *software*.

9. Um satélite de comunicações ou uma ligação de dados recentemente interceptados podem ser analisados utilizando o sistema de caracterização de transmissor-receptor Modelo 196 da AST. Logo que a sua estrutura básica de comunicações tenha sido analisada, o sistema de análise fotográfica de banda larga Modelo 195, também conhecido como SNAPPER, pode gravar dados de amostra mesmo dos sistemas de mais alta capacidade, suficientes para analisar comunicações ao pormenor. No início de 1999, funcionando em conjunto com a unidade flexível de aquisição de dados Modelo 990, este sistema era capaz de gravar, reproduzir e analisar a uma velocidade de dados de até 2,488 Gbps (SONET OC-48). Isto é 16 vezes mais rápido do que as maiores ligações principais utilizadas geralmente na Internet, maior do que a capacidade de telefonia de qualquer satélite de comunicações actual e equivalente a 40 000 telefonemas simultâneos. Pode ser equipado com 48 Gbytes de memória (500-1000 vezes maior do que aquela que se pode encontrar num computador pessoal normal), permitindo gravações relativamente longas de ligações de dados de alta velocidade. A capacidade de 2,5 Gbps de uma só unidade SNAPPER excede a actual velocidade de dados diária máxima encontrada num intercâmbio de Internet de grandes dimensões.[77]

10. Tanto a AST como a IDEAS oferecem uma vasta gama de gravadores, desmultiplexadores, *scanners* (exploradores) e processadores, concebidos

principalmente para processar sinais do tipo europeu (CECT) E-1 e E-3 (entre outros) a velocidades de dados de até 160 Mbps. Os sinais podem ser gravados em bancos de gravadores de fita de alta velocidade ou em redes de disco rígido "RAID"[78] de alta capacidade. Os sinais ópticos interceptados podem ser examinados com o dispositivo de análise SONET da AST, Modelo 257E.

11. Logo que as ligações de comunicação tenham sido analisadas e divididas nas suas partes constituintes, a etapa seguinte da recolha de Comint envolve processadores multi-canal que extraem e filtram as mensagens e os sinais dos canais pretendidos. Existem três grandes categorias de interesse: os canais de voz (canais telefónicos), que normalmente transportam sinais de telefonia; as comunicações por fax e os *modems* de dados analógicos. Existe uma vasta selecção de processadores Comint multi-canal. Quase todos eles separam as mensagens de voz, fax e dados em "correntes" distintas, para serem posteriormente processadas e analisadas.

12. O processador multi-canal Modelo 120 da AST, utilizado pela NSA em configurações diferentes conhecidas como STARQUAKE, COBRA e COPPERHEAD, pode comportar 1.000 canais de voz simultâneos e extrair automaticamente o tráfego de fax, dados e voz. O Modelo 128, ainda maior, pode processar 16 canais E-3 europeus (a uma velocidade de dados de 500 Mbps) e extrair 480 canais de interesse. O gigante da gama da AST em 1999, o desmultiplexador de canais de voz Modelo 132, pode examinar até 56.700 canais de comunicação, extraindo mais de 3.000 canais de voz de interesse. A AST fornece também equipamento de Sigint para interceptar serviços de satélite VSAT[79] de baixa capacidade, utilizados por empresas mais pequenas ou utilizadores domésticos. Estes sistemas podem ser interceptados pelo processador SCPS Modelo 285 da AST, que identifica e extrai até 48 canais de interesse, fazendo a distinção entre voz, fax e dados.

13. Segundo publicações do Governo norte-americano, um sistema inicial de extracção de banda larga foi instalado na estação da NSA em Vint Hill Farms, em 1970, altura em que começou a recolha sistemática de intercepções de COMSAT. Esta estação encontra-se presentemente encerrada. As publicações norte-americanas identificam o Centro Regional de Operação Sigint (Regional Sigint Operations Centre) da NSA/CSS em San Antonio, Texas, como uma unidade que fornece actualmente um serviço de extracção de banda larga multi-canal.

Filtragem, processamento de dados e análise de fac-símile

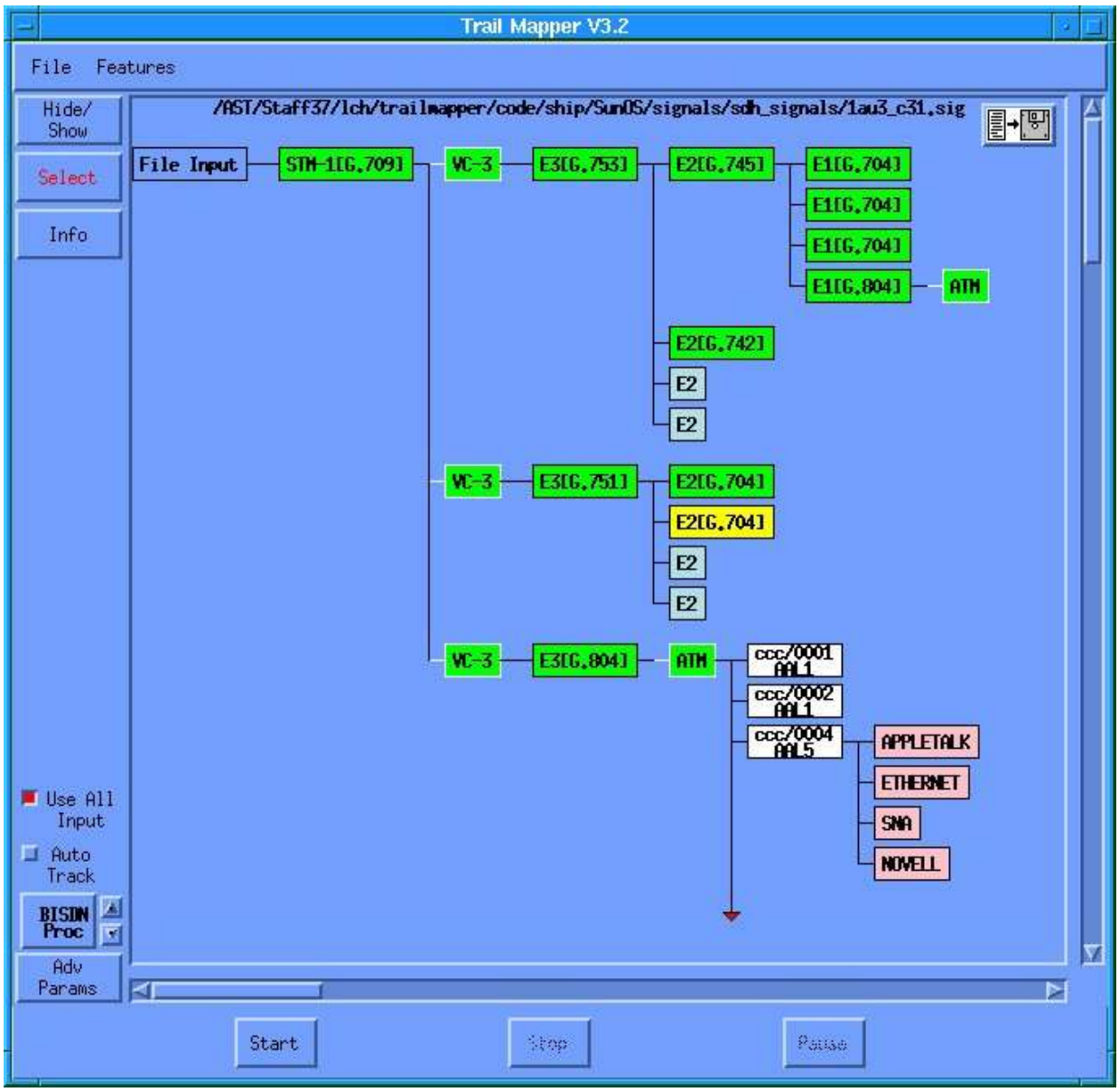
14. Assim que os canais de comunicação tiverem sido identificados e os sinais de interesse tiverem sido extraídos, são analisados por estações de trabalho sofisticadas que utilizam *software* especial. A estação de trabalho para análise de sinais da AST, denominada ELVIRA, é típica deste tipo de equipamento de Sigint. Este sistema, que pode ser utilizado num computador portátil em locais secretos, estuda os canais recebidos e extrai dados de Comint normais, incluindo especificações técnicas (STRUM) e informações acerca dos destinos das chamadas (SRI ou informações relacionadas com os sinais). As comunicações seleccionadas são reenviadas para locais distantes utilizando o formato normal para os (dados de sinais recolhidos CSDF) da NSA.[80]

15. Os sistemas de dados de alta velocidade podem também ser passados para o sistema de *software* TRAILMAPPER da AST, que trabalha a uma velocidade de dados de até 2,5 Gbps. Este sistema pode interpretar e analisar todos os tipos de sistemas de telecomunicações, incluindo os que funcionam segundo as normas europeias, americanas e ópticas. O TRAILMAPPER parece ter sido concebido com vista a analisar comunicações em ATM (modo de transferência assíncrona). O ATM é um moderno sistema de comunicação digital de grande capacidade. É mais adequado do que as ligações de Internet normais para transportar tráfego multimédia e para fornecer redes privadas às empresas (VPN, LAN, ou WAN). O TRAILMAPPER identificará e caracterizará estas redes comerciais.

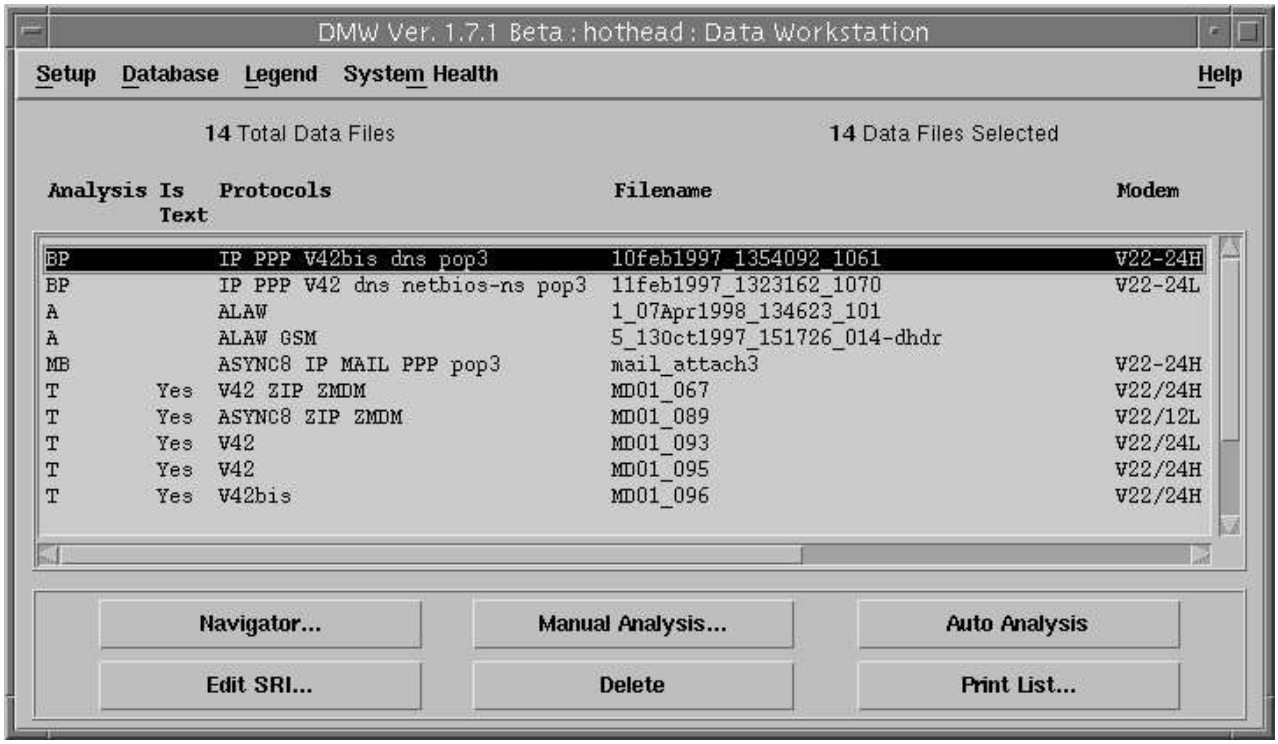
16. Na etapa seguinte a jusante, os sinais interceptados são processados consoante forem de voz, fax ou dados. A estação de trabalho para dados da AST destina-se a categorizar todos os aspectos das comunicações de dados, incluindo sistemas para lidar com correio electrónico ou para enviar ficheiros pela Internet.[81] Embora os sistemas de *modem* mais recentes (excepto o RDIS) não estejam incluídos nas especificações anunciadas, torna-se claro, a partir das investigações publicadas, que a AST desenvolveu a tecnologia para interceptar e processar os mais recentes sistemas de comunicações de dados utilizados por indivíduos e empresas para ter acesso à Internet.[82] A estação de trabalho para dados pode armazenar e processar automaticamente 10 000 sinais gravados diferentes.

17. As mensagens de fax são processadas pela estação de trabalho para imagens de fax da AST. Esta é descrita como uma ferramenta de análise interactiva, de fácil utilização, para um exame rápido das imagens armazenadas no disco. Embora não seja mencionado na literatura da AST, o pré-processamento de fax normal para os computadores Dicionário envolve o *software* automático de "reconhecimento óptico de caracteres" (OCR). Isto transforma o texto de um original em texto passível de ser lido (e processado) pelo computador. A eficácia destes sistemas torna a Comint, com origem em faxes, um importante sub-sistema de recolha. Tem um inconveniente: não existem sistemas informáticos de OCR que reconheçam com segurança o texto manuscrito. Ninguém sabe ao certo como conceber um sistema deste género. Por conseguinte, e adversamente, as mensagens de fax manuscritas podem ser uma forma de comunicação segura que pode escapar aos critérios de vigilância do Dicionário, desde que as informações relacionadas com o sinal a elas associadas (os números de fax do remetente e do destinatário) não sejam reconhecidas como sendo de interesse e enviadas para uma estação de trabalho para imagens de fax.

18. A AST fabrica também um sistema de identificação de aparelhos de chamada de pessoas e de extracção de mensagens que recolhe e processa automaticamente os dados de sistemas de chamada de pessoas comerciais. A IDEAS oferece um processador para vídeo-conferências que pode, simultaneamente, visualizar ou gravar duas sessões de vídeo-conferência simultâneas. Os sistemas de Sigint para interceptar redes de telemóveis, tal como a GSM, não são publicitados pela AST nem pela IDEAS, mas podem ser encontrados noutros fornecedores norte-americanos. As especificações e a imediata disponibilidade desses sistemas indica até que ponto a Comint se tornou industrializada e difusa. Afastou-se muito da era em que (embora erradamente) era publicamente associada apenas à monitorização de mensagens diplomáticas ou militares.



Software "Trailmapper" da NSA mostrando a detecção automática de redes privadas no interior de uma portadora STM-1 de grande capacidade interceptada



O sistema de software da estação de trabalho para dados analisa até 10.000 mensagens gravadas, identificando o tráfego da Internet, mensagens de correio electrónico e anexos

Análise do tráfego, reconhecimento de palavras-chave, recuperação de texto e análise temática

19. A análise do tráfego é um método que serve para obter informação secreta a partir de informações relacionadas com sinais, tal como o número marcado numa chamada telefónica ou os dados de identificação da linha chamadora (CLID), que identificam a pessoa que efectua a chamada. A análise do tráfego pode ser utilizada sempre que o conteúdo da mensagem não esteja disponível, por exemplo, quando a criptografação é utilizada. Ao analisar os padrões das chamadas, é possível analisar e estudar redes de associações pessoais. Isto é um dos principais métodos de análise das comunicações por voz.

20. Sempre que existem comunicações passíveis de serem lidas por máquinas, o reconhecimento de palavras-chave é fundamental para os computadores Dicionário e para o sistema ECHELON. A função do Dicionário é simples. O seu modo básico de funcionamento é semelhante ao motores de busca da Internet. As diferenças residem na substância e na dimensão. Os Dicionários implementam a definição de tarefas da respectiva estação anfitriã em relação a todo o conjunto de comunicações recolhidas e automatizam a distribuição de produto não processado seleccionado.

21. Foram desenvolvidos sistemas avançados para efectuar a classificação a alta velocidade de grandes volumes de informações interceptadas. No final da década de 80, o fabricante dos satélites de Sigint RHYOLITE, a TRW, concebeu e produziu um

microchip para a detecção rápida de dados (Fast Data Finder - FDF) para a NSA. O *chip* FDF deixou de ser secreto em 1972 e ficou disponível para utilização comercial através de uma empresa filiada, a Paracel. Desde então, a Paracel vendeu mais de 150 sistemas de filtragem de informação, muitos dos quais ao Governo norte-americano. A Paracel descreve a sua actual tecnologia de FDF como o sistema de filtragem mais rápido, mais preciso e adaptável do mundo. Segundo esta empresa, uma só aplicação TextFinder pode envolver triliões de *bytes* de arquivos de texto e milhares de utilizadores em linha, ou *gigabytes* de dados em directo por dia que são filtrados em relação a milhares de perfis de interesses complexos. De acordo com a Paracel, o *chip* TextFinder implementa as mais abrangentes funções de comparação de sequências de caracteres de qualquer sistema de recuperação de texto no mundo. Dispositivos como este são ideais para serem utilizados nos sistemas ECHELON e Dicionário.

22. Um sistema de menor capacidade, o processador de reconhecimento de padrões PRP-9800, é fabricado pela IDEAS. Trata-se de uma placa de computador que pode ser aplicada num PC normal. Este processador consegue analisar fluxos de dados de até 34 Mbps (como os da norma europeia E-3), fazendo corresponder cada bit a mais de 1.000 padrões previamente seleccionados.

23. Por muito poderosos que os métodos Dicionário e os motores de busca de palavras-chave possam ser, eles e as enormes bases de dados a eles associadas, poderão tornar-se arcaicos em breve. A **análise de tópicos** é uma técnica mais poderosa e intuitiva, que está a ser desenvolvida e promovida pela NSA com confiança. A análise de tópicos permite que os clientes de Comint peçam aos respectivos computadores que encontrem documentos sobre o assunto X. X pode ser "A paixão de Shakespeare" ou "Armamento para o Irão".

24. Num teste norte-americano padrão utilizado para avaliar os sistemas de análise de tópicos,[83] uma das tarefas que o programa recebe é a de encontrar informações acerca de "subsídios da Airbus". A abordagem tradicional envolve o fornecimento ao computador de termos-chave, outros dados relevantes e sinónimos. Neste exemplo, as designações A-300 ou A-320 podem ser sinónimos de "Airbus". A desvantagem desta abordagem consiste no facto de poder encontrar informação secreta irrelevante (por exemplo, relatórios sobre subsídios de exportação para bens transportados num Airbus) e não encontrar material relevante (por exemplo, uma análise financeira de uma empresa no consórcio que não menciona o produto Airbus pelo nome). A análise de tópicos ultrapassa este problema e equipara-se melhor à inteligência humana.

25. O principal impulso detectável da investigação da NSA sobre a análise de tópicos centra-se num método denominado análise N-gram. Desenvolvida no seio do grupo de investigação da NSA, responsável pela automatização da Sigint, a análise N-gram é um método rápido e geral de classificar e recuperar texto passível de ser lido por máquinas consoante o idioma e/ou o tópico. Afirma-se que o sistema N-gram funciona independentemente do idioma utilizado ou do tópico estudado. A NSA obteve a patente deste método em 1995.[84]

26. Para utilizar a análise N-gram, o operador ignora palavras-chave e define a procura fornecendo ao sistema documentos escritos seleccionados sobre o tópico de interesse. O sistema determina qual é o tópico a partir do grupo de documentos e depois calcula a probabilidade de outros documentos abordarem o mesmo tópico. Em 1994, a NSA disponibilizou o sistema N-gram para exploração comercial. O grupo de

investigação da NSA afirmou que este poderia ser utilizado em conjuntos de dados muito grandes (milhões de documentos), poderia ser rapidamente implementado em qualquer sistema informático e que poderia trabalhar eficazmente com textos que contivessem muitos erros (normalmente 10 a 15% de todos os caracteres).

27. Segundo o ex-director da NSA William Studeman, a gestão de informações será o problema mais importante para a comunidade da espionagem (dos Estados Unidos) no futuro.[85] Explicando esta afirmação em 1992, ele descreveu o tipo de filtragem envolvida em sistemas como o ECHELON. Segundo ele, um sistema de recolha de informação não identificado pode gerar milhões de entradas em cada meia hora, os filtros só seleccionam cerca de 6.500 entradas e apenas 1.000 correspondem aos critérios de reencaminhamento. Destas, 10 são normalmente seleccionadas por analistas, sendo produzido um só relatório. De acordo com William Studeman, trata-se de estatísticas rotineiras para vários sistemas de recolha e análise de informações secretas que recolhem informações técnicas secretas.

Sistemas de reconhecimento de voz

28. Durante mais de 40 anos, a NSA, a ARPA, o GCHQ e a Joint Speech Research Unit do Governo britânico realizaram e patrocinaram investigações sobre o reconhecimento da voz. Muitos relatos na imprensa (e o relatório anterior do STOA) sugeriram que essas investigações forneceram sistemas que podem seleccionar automaticamente comunicações por telefone com interesse em termos de informação secreta, com base na utilização de determinadas palavras-chave pelo orador. Se existissem, esses sistemas permitiriam que se recolhesse muito mais informação Comint a partir de conversas telefónicas do que com outros métodos de análise. A afirmação de que existem sistemas de detecção de palavras pelo telefone parece ser apoiada pela recente disponibilização de uma gama de produtos de *software* de baixo custo resultantes desta investigação. Estes produtos permitem que os utilizadores de PC ditem para o computador em vez de introduzirem dados através do teclado.[86]

29. O problema é que nas aplicações de Comint, ao contrário dos produtos de ditado para computadores pessoais, os sistemas de reconhecimento da voz têm de trabalhar num ambiente de vários oradores e de vários idiomas, onde numerosos oradores nunca antes ouvidos podem ter diferenças fisiológicas, variações nos dialectos e traços de fala. Os sistemas de PC comerciais normalmente requerem uma ou mais horas de treino para poderem reconhecer um só orador de forma fiável. Mesmo depois deste treino, esses sistemas podem errar na transcrição de 10% ou mais das palavras proferidas.

30. Nas aplicações de ditado para PC, o orador pode corrigir os erros de transcrição e treinar continuamente o sistema de reconhecimento, tornando uma taxa de erro moderada aceitável. Para utilização em Comint, em que o sistema de intercepção não tem conhecimento prévio do que foi dito (nem sequer do idioma utilizado) e que tem de funcionar num ambiente de canal fraco, como um canal telefónico, essas taxas de erro são inatingíveis. Mas pior do que isso, mesmo as taxas de erro moderadas podem inutilizar um sistema de reconhecimento de palavras-chave ao criar falsos resultados positivos (palavras erradamente identificadas como palavras-chave) bem como falsos negativos (ignorar palavras-chave genuínas).

31. Este estudo não encontrou qualquer prova de que os sistemas de reconhecimento de palavras-chave através da voz estejam actualmente operacionais, nem de que sejam suficientemente exactos para que valha a pena utilizá-los para fins de espionagem.

Reconhecimento de voz em contexto

32. A técnica fundamental em muitas aplicações de reconhecimento da voz é um método estatístico denominado modelos de Markov não-observáveis (HMM). Os sistemas HMM foram desenvolvidos em muitos centros e, academicamente, diz-se que proporcionam um bom desempenho em termos de detecção de palavras, utilizando pouco ou nenhum treino acústico da voz.[87] A equipa que relatou este resultado testou o sistema utilizando dados do quadro comutador telefónico do Departamento de Defesa dos Estados Unidos, que continha gravações de milhares de conversas telefónicas diferentes ocorridas nos Estados Unidos. Num teste limitado, as probabilidades de detectar correctamente as ocorrências de 22 palavras-chave iam de 45 a 68% em condições que permitiam 10 resultados positivos falsos por palavra-chave e por hora. Desta forma, se aparecessem 1.000 palavras-chave genuínas durante uma conversa de uma hora, o sistema falharia pelo menos 300 e teria dado 220 alarmes falsos.

33. Por volta da mesma altura (Fevereiro de 1990, a CSE, organização de Sigint canadiana, adjudicou a uma empresa de consultoria informática com sede em Montreal o primeiro de uma série de contratos para desenvolver um sistema de detecção de palavras em Comint.[88] O objectivo do projecto era o de construir um detector de palavras que funcionasse bem, mesmo com chamadas ruidosas. Três anos mais tarde, o CRIM relatou que a experiência lhes tinha ensinado que, independentemente das condições ambientais, a detecção de palavras continuava a ser um problema difícil. O problema principal, que é conhecido por todos os ouvintes, é que uma só palavra ouvida por si só pode ser facilmente mal interpretada, enquanto no discurso em contexto, o significado pode ser deduzido a partir das restantes palavras. O CRIM concluiu em 1993 que era provável que a maneira mais eficaz de construir um detector de palavras fiável fosse construindo um sistema de reconhecimento de discurso em contexto (CSR) com um grande vocabulário.

34. O *software* de reconhecimento de discurso em contexto a funcionar em tempo real necessita de um processador rápido, com uma grande potência. Devido à falta de treino e ao ambiente complexo dos sinais encontrado em chamadas telefónicas interceptadas, é provável que mesmo processadores mais rápidos e com melhor *software* que os utilizados nos PC modernos tivessem piores resultados do que aqueles presentemente produzidos por sistemas comerciais bem treinados. Um problema subjacente importante é que o reconhecimento de palavras-chave na voz é, tal como com as mensagens que podem ser lidas por máquinas, um meio imperfeito para um fim muito mais útil em termos de espionagem - a **detecção de tópicos**.

35. Em 1993, tendo fracassado na construção de um detector de palavras funcional, o CRIM sugeriu "contornar" o problema e tentar desenvolver um detector de tópicos na voz. O CRIM afirmou que as experiências preliminares relatadas numa reunião recente dos fornecedores americanos no campo da defesa tinham indicado que esta poderia ser, de facto, uma excelente forma de abordar o problema. Ofereceram-se para produzir um sistema de detecção de tópicos operacional até 1995, mas não o conseguiram fazer. Quatro anos mais tarde, ainda estavam a experimentar o modo

como poderiam construir um detector de tópicos por voz.[89] Foi-lhes adjudicado mais um contrato de investigação. Um dos métodos propostos pelo CRIM era a técnica N-gram da NSA.

Identificação do orador e outras técnicas de selecção de mensagens de voz

36. Em 1993, o CRIM comprometeu-se também em fornecer à CSE um módulo operacional de identificação do orador até Março de 1995. Nada mais foi dito acerca deste projecto, o que sugere que o objectivo pode ter sido alcançado. No mesmo ano, segundo documentos da NSA, a empresa IDEAS forneceu um dispositivo de detecção e análise de actividades de voz, Modelo TE464375-1, aos departamentos da NSA na unidade de Cheltenham do GCHQ. A unidade formava o centro de um sistema de monitorização da voz assistido por computador com 14 posições. Este poderá ter sido também um sistema inicial de identificação do orador.

37. Em 1995, relatórios muito citados sugeriam que o sistema de identificação do orador da NSA tinha sido utilizado para ajudar a capturar Pablo Escobar, líder de um cartel de droga. Os relatórios eram muito semelhantes a um romance de Tom Clancy, o que sugere que a história pode dever-se mais a Hollywood do que à alta tecnologia. Em 1997, a CRE canadiana adjudicou um contrato a outro investigador para que este desenvolvesse novos algoritmos de recuperação para as características da voz utilizadas para a identificação de oradores, sugerindo que este método não era ainda uma tecnologia totalmente amadurecida. Segundo pessoal que trabalha em Sigint e que está familiarizado com a actual utilização do Dicionário, este pode ser programado para tentar identificar oradores específicos em canais telefónicos. Mas a identificação do orador ainda não é uma técnica de Comint particularmente fiável ou eficaz.[90]

38. Na ausência de técnicas eficazes de detecção de palavras ou de identificação do orador, a NSA procurou meios alternativos para analisar automaticamente comunicações telefónicas. Segundo o guia de classificação da NSA, as outras técnicas analisadas incluem a detecção da voz, que consiste em detectar a presença ou ausência de actividade da voz; a discriminação do orador, composta por técnicas para fazer a distinção entre a voz de dois ou mais oradores; e o cálculo da legibilidade, que consiste em técnicas para determinar a qualidade dos sinais de voz. As descrições dos sistemas têm de ser classificadas como "secretas" se a NSA determinar que elas representam grandes avanços em relação a técnicas conhecidas na comunidade de investigação.[91]

"Redução do factor trabalho": a subversão dos sistemas criptográficos

39. De 1940 até à data, a NSA tem minado a eficácia dos sistemas criptográficos fabricados ou utilizados na Europa. O alvo mais importante da actividade da NSA era uma empresa suíça proeminente, a Crypto AG. Esta firma estabeleceu uma forte posição como fornecedora de sistemas de códigos e de cifras após a Segunda Guerra Mundial. Muitos governos não confiavam em produtos vendidos por grandes potências. Por outro lado, as empresas suíças neste sector beneficiaram da neutralidade e imagem de integridade da Suíça.

40. A NSA conseguiu manobrar fraudulentamente os sistemas de criptografação vendidos pela Crypto AG, permitindo às agências da UKUSA ler o tráfego diplomático e militar codificado de mais de 130 países. A intervenção secreta da NSA foi conseguida

através do dono e fundador da empresa, Boris Hagelin, e envolvia visitas periódicas à Suíça feitas por "consultores" norte-americanos ao serviço da NSA. Um deles era Nora L. MacKabee, funcionária da NSA. Um jornal dos Estados Unidos obteve cópias de documentos confidenciais da Crypto AG que relatavam a presença de MacKabee em reuniões decorridas em 1975, onde se discutia a concepção de uma nova máquina da Crypto AG.[92]

41. A finalidade das intervenções da NSA era a de garantir que, apesar de os sistemas de codificação parecerem seguros para outros criptólogos, de facto não o eram. Cada vez que uma máquina era utilizada, os respectivos utilizadores seleccionavam uma longa chave numérica, que era alterada periodicamente. Naturalmente, os utilizadores desejavam escolher as suas próprias chaves, desconhecidas para a NSA. Se se pretendia que as máquinas da Crypto AG parecessem fortes para examinadores externos, o respectivo sistema de codificação deveria funcionar e ser realmente forte. A solução da NSA para este problema aparente consistia em conceber a máquina de modo a que transmitisse aos ouvintes a chave que estava a utilizar. Para evitar que outros ouvintes reconhecessem o que estava a acontecer, a própria chave tinha também de ser enviada em código, um código diferente, conhecido apenas pela NSA. Consequentemente, cada vez que a NSA ou o GCHQ interceptavam uma mensagem enviada através da utilização destas máquinas, leriam primeiro a sua parte codificada da mensagem, o chamado "*hilfsinformationen*" (campo de informações de ajuda) e extrairiam a chave que o alvo estava a utilizar. Nessa altura, conseguiriam ler a mensagem tão ou mais rapidamente do que o destinatário pretendido.[93]

42. A mesma técnica foi reutilizada em 1995, quando a NSA ficou preocupada com os sistemas de segurança criptográficos que estavam a ser incorporados pela Microsoft, pela Netscape e pela Lotus no *software* de Internet e correio electrónico. As empresas concordaram em adaptar o *software* de forma a reduzir o nível de segurança facultado aos utilizadores fora dos Estados Unidos. No caso do Lotus Notes, que inclui um sistema de correio electrónico seguro, o sistema criptográfico incorporado utiliza uma chave de criptografação de 64 bits. Isto faculta um nível de segurança médio que, hoje em dia, provavelmente só poderá ser quebrado pela NSA no espaço de meses ou anos.

43. A Lotus incorporou uma passagem secreta de "informações de ajuda" para a NSA no sistema Notes, conforme o governo sueco descobriu em 1997, para seu embaraço. Até então, o sistema era utilizado diariamente para envio de correio confidencial por deputados suecos, 15.000 funcionários das finanças e 400.000 a 500.000 cidadãos. O Lotus Notes inclui um "campo de redução do factor trabalho" (WRF - workfactor reduction field) em todas as mensagens de correio electrónico enviadas por utilizadores do sistema que não sejam dos Estados Unidos. Tal como o seu antecessor, o "campo de informações de ajuda" da Crypto AG, este dispositivo diminui a dificuldade da NSA na leitura de correio electrónico europeu e de outros países, deixando de ser um problema praticamente insolúvel para ser apenas o trabalho de alguns segundos. O WRF transmite 24 dos 64 *bits* da chave utilizada para cada comunicação. O WRF é codificado utilizando um sistema de "chave pública" que só pode ser lido pela NSA, o que é admitido pela Lotus, empresa subsidiária da IBM. A empresa disse ao jornal *Svenska Dagbladet* que a diferença entre a versão americana e a versão para exportação do Notes consiste nos níveis de criptografação. Segundo a empresa, entregam chaves de 64 bits a todos os clientes, mas 24 destes *bits*, na versão fornecida fora dos Estados Unidos, ficam depositados no Governo americano.[94]

44. Dispositivos semelhantes são incorporados em todas as versões para exportação dos *browsers* da Internet fabricados pela Microsoft e pela Netscape. Ambas as empresas utilizam uma chave normal de 128 bits. Na versão para exportação, esta chave não é reduzida. Em vez disso, 88 bits da chave são transmitidos com cada mensagem, permanecendo secretos 40 bits. Por conseguinte, praticamente todos os computadores na Europa possuem, como função incorporada de série, um sistema de redução do factor trabalho da NSA para que esta possa (por si só) descobrir o código do utilizador e ler mensagens seguras.

45. A utilização de sistemas de criptografação potentes e eficazes irá limitar, cada vez mais, a capacidade das agências de Comint de **processar** a informação recolhida. A "lei de Moore" indica que o custo do poder informático é reduzido para metade cada cada 18 meses. Isto afecta tanto as agências como os respectivos alvos. Os computadores baratos conseguem agora efectuar eficientemente cálculos matemáticos complexos, necessários para uma criptografia eficaz. Na ausência de novas descobertas no campo da física ou da matemática, a lei de Moore favorece os criadores de código e não aqueles que os descodificam.

Glossário e definições

HF	Alta frequência; frequências entre 3 MHz e 30 MHz.
Análise do tráfego	Em Sigint, método de análise e de obtenção de informação secreta a partir de mensagens sem referência ao respectivo conteúdo; por exemplo, ao estudar a origem e o destino de mensagens, tendo em vista a clarificação da relação entre o remetente e o destinatário, ou grupos de destinatários.
Análise N-gram	Sistema para analisar documentos de texto; neste contexto, trata-se de um sistema para fazer corresponder um grande grupo de documentos a um grupo menor com o mesmo tópico de interesse. O método depende da contagem das ocorrências de grupos de caracteres de comprimento N em cada documento; é por este facto que se chama N-gram.
ATM	Modo de transferência assíncrona; forma de comunicação digital de alta velocidade cada vez mais utilizada na Internet.
BND	Bundesnachrichtendienst; agência de informação secreta estrangeira da República Federal da Alemanha. As suas funções incluem a Sigint.
CCITT	Comissão Consultiva Internacional Telegráfica e Telefónica; agência das Nações Unidas que desenvolve normas e protocolos para as telecomunicações; parte da UIT; também conhecida como UIT-T.
CECT	Conferência Europeia dos Correios e Telecomunicações
CLID	Calling Line Identification Data (dados de identificação da linha chamadora)
Comint	Espionagem de comunicações
COMSAT	Satélite de comunicações (civil/comercial); para utilização no campo das comunicações militares, o termo é frequentemente invertido, ou seja, SATCOM.
CRIM	Centre de Recherche Informatique de Montreal (Centro de Investigação Informática de Montreal)
CSDF	Collected Signals Data Format (formato para os dados de sinais recolhidos); termo utilizado apenas em Sigint.
CSE	Communications Security Establishment, agência de Sigint canadiana
CSS	Central Security Service, componente militar da NSA
CTT	Correios, Telégrafos e Telefones (administração ou autoridade)
DARPA	Defense Advanced Research Projects Agency (Departamento da Defesa dos Estados Unidos)
DGSE	Direction Générale de Sécurité Extérieure, agência francesa de informação estrangeira. As suas funções incluem a Sigint.
DSD	Defence Signals Directorate, agência de Sigint australiana da Commonwealth
DODJOCC	Department of Defense Joint Operations Centre Chicksands
E1, E3 (etc.)	Norma para os sistemas de comunicação digitais ou TDM definida pela CECT e utilizada principalmente na Europa e fora da América do Norte
ENFOPOL	Designação da EU para os documentos relativos a questões de aplicação da lei/polícia
FAPSI	Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii, agência federal russa para as comunicações governamentais e a informação. As suas funções incluem a Sigint.
FBI	Agência Federal de Investigação, agência nacional de aplicação da lei e de contra-espionagem dos Estados Unidos
FDF	Fast Data Finder (detector rápido de dados)
FDM	Multiplex por divisão de frequência, uma forma de comunicação multi-canal com base em sinais analógicos
FISA	Foreign Intelligence Surveillance Act (Estados Unidos)
FISINT	Foreign Instrumentation Signals Intelligence (espionagem de sinais de instrumentação estrangeiros), terceiro ramo da Sigint
Gbps	Gigabits por segundo
GCHQ	Quartel-General de Comunicações do Governo, agência de Sigint do Reino Unido
GHz	GigaHertz
HDLC	High-level Data Link Control (controlo de ligações de dados de alto nível)
HMM	Modelos de Markov não-observáveis, técnica vastamente utilizada em sistemas de reconhecimento de voz
ILETS	International Law Enforcement Telecommunications Seminar (Seminário Internacional sobre a Vigilância Legal das Telecomunicações)
Intelsat	Satélite internacional de telecomunicações
IOSA	Interim Overhead Sigint Architecture (arquitectura de Sigint aérea integrada)
Iridium	Sistema de comunicações pessoais por satélite que envolve 66 satélites numa órbita baixa da terra e que fornece comunicações globais a partir de telemóveis
ISP	Fornecedor de serviços Internet
IUR	Requisitos dos utilizadores internacionais (para a intercepção de comunicações); o IUR 1.0 foi preparado pelo ILETS (*qv*) em 1994
IXP	Ponto de intercâmbio da Internet
LAN	Rede de área local
LEA	Law Enforcement Agency (utilização nos Estados Unidos, significa agência de aplicação da lei)
Mbps	Megabits por segundo
MHz	MegaHertz

Microondas	Sinais de rádio com comprimentos de onda de 10 cm ou menos; frequências acima de 1 GHz
Modem	Dispositivo para enviar dados de e para (por exemplo) um computador; um "modulador-desmodulador".
MIME	Multipurpose Internet Message Extension; sistema utilizado para enviar ficheiros de computador, imagens, documentos e programas como "anexos" de uma mensagem de correio electrónico.
NSA	Agência de Segurança Nacional, agência de Sigint dos Estados Unidos
OCR	Reconhecimento Óptico de Caracteres
PC	Computador pessoal
PCS	Sistemas de comunicações pessoais; o termo inclui sistemas de telemóveis, de aparelhos de chamada de pessoas e futuras ligações de dados de rádio de área ampliada para computadores pessoais, etc..
POP (ou POP3)	Post Office Program; sistema utilizado para receber e reter correio electrónico.
RAID	Conjuntos redundantes de discos baratos
RDIS	Rede Digital com Integração de Serviços
SCI	Informação compartimentada sensitiva; utilizada para limitar o acesso a informações de Comint segundo "compartimentos".
SCPC	Canal único por portadora; sistema de comunicações por satélite de pouca capacidade
SMTP	Standard Mail Transport Protocol
Sigint	Informação sobre sinais
Síntese	Em Sigint, é a tarefa analítica de substituir um texto integral pelo seu sentido ou pelos pontos principais de uma comunicação
SONET	Rede óptica síncrona
SMDS	Switched Multi-Megabit Data Service
SMO	Support for Military Operations (apoio a operações militares)
SPCS	Sistemas de comunicações pessoais via satélite
SRI	Signal Related Information (informação relacionada com sinais); termo utilizado apenas em Sigint
STOA	Gabinete de avaliação das opções científicas e técnicas do Parlamento Europeu; entidade que solicitou este relatório
T1, T3 (etc.)	Sistemas de comunicações digitais ou TDM inicialmente definidos pelo sistema telefónico Bell na América do Norte, onde é principalmente utilizado.
TCP/IP	Terminal Control Protocol/Internet Protocol
TDM	Multiplex por divisão de tempo; forma de comunicação multi-canal normalmente baseada em sinais digitais
UIT	União Internacional das Telecomunicações
UKUSA	Acordo entre o Reino Unido e os Estados Unidos da América
VPN	Rede privada virtual
VSAT	Terminal de muito pequena abertura; sistema de comunicações por satélite de pouca capacidade que serve utilizadores domésticos e comerciais
WAN	Rede de área amplificada
WRF	Workfactor Reduction Field (campo de redução do factor trabalho)
WWW	World Wide Web

X.25, V.21, V.34, V.90, V.100 (etc.) são normas de telecomunicações da CCITT

Ilustrações: página 5: Força Aérea dos Estados Unidos; IPTV Ltd; página 6: Stephen King, Charles V. Pick; IPTV Ltd; página 8: Jim Bamford, GCHQ; página 9: Marinha dos Estados Unidos, KGB/Serviços de segurança russos; página 12: D. Campbell.

Notas

[1] UKUSA refere-se ao acordo assinado em 1947 entre o Reino Unido e os Estados Unidos, relativo a espionagem de sinais. As nações da aliança UKUSA são os Estados Unidos (os "primeiros contratantes"), o Reino Unido, o Canadá, a Austrália e a Nova Zelândia (os "segundos contratantes").
[2]An appraisal of the Technologies of Political Control", Steve Wright, Omega Foundation, Parlamento Europeu (STOA), 6 de Janeiro de 1998.
[3] "They've got it taped", Duncan Campbell, *New Statesman*, 12 de Agosto de 1988. "Secret Power: New Zealand's Role in the International Spy Network", Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, Nova Zelândia, 1996.
[4] Directiva n.º 6 sobre espionagem, do Conselho Nacional de Segurança dos Estados Unidos, 17 de Fevereiro de 1972 (primeira edição em 1952).
[5] SIGINT encontra-se actualmente definida como sendo composta por COMINT, ELINT (espionagem de comunicações electrónicas ou não) e FISINT (espionagem de sinais de instrumentação estrangeiros).
[6] Segundo declaração de Martin Brady, Director da DSD, a 16 de Março de 1999, transmitida no programa *Sunday Programme* do Channel 9 (televisão australiana), de 11 de Abril de 1999.
[7] "Farewell", despacho enviado a todo o pessoal da NSA, William Studeman, 8 de Abril de 1992. As duas áreas comerciais que Studeman referia eram o maior acesso global e o apoio a operações militares.
[8] *Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii*, Agência Federal (Russa) para as comunicações e informações governamentais. As funções da FAPSI alargam-se para além da Comint e incluem o fornecimento de sistemas de comunicação governamentais e comerciais.
[9] Comunicações privadas de antigos funcionários da NSA e do GCHQ.
[10] Sensitive Compartmented Intelligence (informação compartimentada sensitiva).
[11]Consultar a nota 1.
[12] Comunicações privadas de antigos funcionários do GCHQ; a lei americana é o Foreign Intelligence Surveillance Act (FISA).
[13] Consultar a nota 6.
[14] Em 1919, as empresas de telecomunicações por cabo comerciais dos Estados Unidos tentaram resistir às exigências por parte do Governo britânico para o acesso a todos os cabos enviados para o estrangeiro. Três destas empresas testemunharam perante o Senado norte-americano sobre estas práticas, em Dezembro de 1920. Neste mesmo ano, o Governo britânico introduziu legislação (o Official Secrets Act, 1920, Secção 4) que facultava acesso a toda e qualquer classe específica de comunicação. Este mesmo poder foi recodificado em 1985, facultando o acesso legal para fins de Comint, a todas as comunicações externas, definidas como todas as comunicações enviadas ou recebidas fora do Reino Unido (Interception of Communications Act, 1984, Secção 3(2)). Nas leis dos outros países da UKUSA são estipulados requisitos semelhantes relativamente aos operadores de telecomunicações. Consulte também "Operação SHAMROCK" (secção 3).
[15] "The Puzzle Palace", James Bamford, Houghton Mifflin, Boston, 1982, p. 331.
[16] Comunicações pessoais de antigos funcionários da NSA e do GCHQ.
[17] "Dispatches: The Hill", transmitido pelo Channel 4 (Reino Unido), 6 de Outubro de 1993. DODJOCC significava Department of Defence Joint Operations Centre Chicksands.
[18] "The Justice Game", Geoffrey Robertson, Capítulo 5, Chatto and Windus, Londres, 1998.
[19] Relatório Fink para o Comité Interno sobre as operações do governo, 1975, citado em "NSA spies on the British government", *New Statesman*, 25 de Julho de 1980.
[20] "Amerikanskiye sputniki radioelektronnoy razvedki na Geosynchronnykh orbitakh" (satélites de Sigint geosincrónicos americanos), Major A. Andronov, *Zarubezhnoye Voyennoye Obozreniyae,* N.º 12, 1993, p. 37-43.
[21] "Space collection" em The US Intelligence Community (quarta edição), Jeffrey Richelson, Westview, Boulder, Colorado, 1999, páginas 185-191.
[22] Consultar a nota 18.
[23] Richelson, *op cit*.
[24] "UK Eyes Alpha", Mark Urban, Faber and Faber, Londres, 1996 p. 56-65.
[25] Para além das estações mencionadas, uma importante estação terrestre cujos alvos incluíam anteriormente os COMSAT soviéticos encontra-se em Misawa, no Japão. Podem encontrar-se estações mais pequenas em Cheltenham, Inglaterra, e em Shoal Bay, Austrália.
[26] "Sword and Shield: The Soviet Intelligence and Security Apparatus", Jeffrey Richelson, Ballinger, Cambridge, Massachusetts, 1986.
[27] "Les Français aussi écoutent leurs alliés", Jean Guisnel, *Le Point*, 6 de Junho de 1998.
[28] *Intelligence* (Paris), 93, 15 de Fevereiro de 1999, p. 3.
[29] "Blind mans Bluff: the untold story of American submarine espionage", Sherry Sontag e Christopher Drew, Public Affairs, Nova Iorque, 1998.
[30] *Ibid*.
[31] *Ibid*.
[32] Um espécimen do equipamento de escuta IVY BELLS encontra-se no museu da antiga KGB em Moscovo. Foi utilizado num cabo que ia de Moscovo até uma instituição científica e técnica nas proximidades.
[33] TCP/IP. TCP/IP significa Terminal Control Protocol/Internet Protocol. IP é a camada de rede básica da Internet.

[34] *Website* do GCHQ no endereço http://www.gchq.gov.uk/technol.html.
[35] Comunicação pessoal da DERA. Um Terabyte é equivalente a mil Gigabytes, ou seja, 1012 bytes.
[36] Comunicação pessoal de John Young.
[37] "Puzzle palace conducting internet surveillance", Wayne Madsen, Computer Fraud and Security Bulletin, Junho de 1995.
[38] *Ibid*.
[39] "More Naked Gun than Top Gun", Duncan Campbell, *Guardian*, 26 de Novembro de 1997.
[40] "Spyworld", Mike Frost e Michel Gratton, Doubleday Canada, Toronto, 1994.
[41] A Agência de Segurança Nacional e os direitos da Quarta Emenda, audições perante a comissão de selecção para estudar as operações governamentais no que diz respeito às actividades de informação, Senado dos Estados Unidos, Washington, 1976.
[42]Carta do Tenente General Lew Allen, director da NSA, ao Procurador norte-americano General Elliot Richardson, 4 de Outubro de 1973; contida no documento anterior.
[43]Comunicação privada.
[44]World in Action, Granada TV.
[45]Estas disposições parecem ser uma tentativa de cumprir as restrições legais da lei relativa à intercepção de comunicações (Interception Communications Act) de 1985, que proíbe o GCHQ de processar mensagens excepto aquelas identificadas em "certificados" governamentais que descrevam o material interceptado que deverá ser examinado. A lei especifica que o material interceptado que não esteja identificado pelo certificado não deverá ser lido, visto ou ouvido por qualquer pessoa. Parece que, embora todas as mensagens que passem pelo Reino Unido sejam interceptadas e enviadas à delegação de Londres do GCHQ, a organização considera que, pelo facto de ser pessoal da British Telecom a operar o computador Dicionário, o controlo do material interceptado ainda cabe ao operador da rede de telecomunicações, a não ser que seja seleccionado pelo Dicionário e passe da BT para o GCHQ.
[46]Comunicações privadas
[47]"Naval Security Group Detachment, Sugar Grove History for 1990", Marinha dos Estados Unidos, 1 de Abril de 1991.
[48]"Missions, functions and tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia" (Missões, funções e tarefas da actividade do Naval Security Group), NAVSECGRU INSTRUCTION C5450.48A, 3 de Setembro de 1991.
[49]Relatório sobre as tarefas do Destacamento 3, 554 Air Intelligence Group, *Air Intelligence Agency Almanac*, Força Aérea dos Estados Unidos, 1998-99.
[50]*Ibid.*, Destacamento 2, 544 Air Intelligence Group.
[51]Informações obtidas por Bill Robinson, Conrad Grebel College, Waterloo, Ontário. Os documentos das CDF e da CFS foram obtidos ao abrigo da lei da liberdade de informação ou publicados na World Wide Web.
[52]Resumo do currículo de Patrick D. Duguay, publicado em http://home.istar.ca/~pdduguay/resume.htm.
[53]Relatório financeiro da CSE, 1 de Março de 1996, editado ao abrigo da lei da liberdade de informação. Não foram fornecidos pormenores adicionais sobre o "ECHELON". É, portanto, ambíguo relativamente ao facto de as despesas serem destinadas ao sistema informático ECHELON ou a funções diferentes (por exemplo, telecomunicações ou serviços de electricidade).
[54]"Secret Power" *op cit*.
[55]*Twenty/Twenty*, TV3 (Nova Zelândia), Outubro de 1999.
[56]Entrevista com David Herson, chefe do grupo de altos-funcionários para a segurança da informação, UE, feita por pessoal da *Engineering Weekly* (Dinamarca), 25 de Setembro de 1996. Publicada em http://www.ing.dk/arkiv/herson.htm.
[57]Resolução do Conselho relativamente à intercepção legal de telecomunicações, 17 de Janeiro de 1995 (96C_329/01).
[58]"International Harmonisation of Technical Requirements for Legal Interception of Telecommunications" (harmonização internacional dos requisitos técnicos para a intercepção legal de telecomunicações), Resolução 1115, Décima reunião plenária do Conselho da UIT, Genebra, 27 de Junho de 1997.
[59]ENFOPOL 98, projecto de resolução do Conselho relativamente à intercepção de telecomunicações com novas tecnologias. Submetido pela Presidência austríaca. Bruxelas, 3 de Setembro de 1998.
[60]ENFOPOL 19, 13 de Março de 1999.
[61]Parlamento Europeu, 14 de Setembro de 1998.
[62]"Uncle Sam's Eavesdroppers", Close Up North, BBC North, 3 de Dezembro de 1998; relatado em "Star Wars strikes back", *Guardian*, 3 de Dezembro de 1998.
[63]Dispatches: The Hill", Channel 4 (Reino Unido), 6 de Outubro de 1993.
[64]*Ibid*.
[65]"Mixing business with spying; secret information is passed routinely to U.S.", Scott Shane, *Baltimore Sun*, 1 de Novembro de 1996.
[66]"UK Eyes Alpha", *op cit*, p. 235.
[67]Comunicação privada.
[68]Consultar a nota 62.
[69]Comunicado à imprensa da Raytheon Corp., publicada em http://www.raytheon.com/sivam/contract.html.
[70]"America's Fortress of Spies", Scott Shane e Tom Bowman, Baltimore Sun, 3 de Dezembro de 1995.
[71]"Company Spies", Robert Dreyfuss, *Mother Jones*, Maio/Junho de 1994.
[72]*Financial Post*, Canadá, 28 de Fevereiro de 1998.
[73]Parlamento Europeu, 16 de Setembro de 1998.
[74]Consultar nota 56.
[75]As comunicações equivalentes podem ser conhecidas como sinais de módulo de transporte síncrono (STM) na hierarquia digital síncrona (norma UIT), como sinais de transporte síncrono (STS) no sistema SONET norte-americano ou como sinais de transportador óptico (OC).
[76]As informações acerca destes sistemas de Sigint foram retiradas de fontes abertas (apenas).

[77]Em Abril de 1999, a velocidade máxima de dados em MAE West era inferior a 1,9 Gbps.
[78]Conjuntos redundantes de discos baratos.
[79]Terminal de muito pequena abertura; SCPC significa canal único por portadora.
[80]"Collected Signals Data Format" (formato para dados de sinais recolhidos); definido na directiva norte-americana relativa a informação sobre sinais n.º 126 e no manual de CSDF da NSA. Duas outras publicações da NSA que fornecem uma orientação adicional são o "Voice Processing Systems Data Element Dictionary" (dicionário de elementos de dados de sistemas de processamento de voz) e o "Facsimile Data Element Dictionary" (dicionário de elementos de dados de fac-símile), ambos publicados em Março de 1997.
[81]A estação de trabalho para dados processa os protocolos TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100 e de *modem*, até ao protocolo V.42 inclusive (consultar glossário).
[82]"Practical Blind Demodulators for high-order QAM signals", J. R. Treichler, M. G. Larimore e J. C. Harp, *Proc IEEE*, **86**, 10, 1998, p. 1907. Treichler é director técnico da AST. O documento descreve um sistema utilizado para interceptar sinais V.34 múltiplos, ampliável aos protocolos mais recentes.
[83]As tarefas foram definidas na segunda conferência sobre recuperação de textos (TREC) organizada pela ARPA e pelo US National Institute of Science and Technology (NIST), em Gaithersburg, Maryland. A 7ª conferência anual sobre TREC ocorreu em Maryland, em 1999.
[84]"Method of retrieving documents that concern the same topic" (Método de recuperação de documentos relativos ao mesmo tópico), número de patente dos Estados Unidos 5418951, emitida a 23 de Maio de 1995; inventor, Marc Damashek; direitos atribuídos à NSA.
[85]Intervenção no simpósio "National Security and National Competitiveness: Open Source Solutions" pelo Vice-Almirante William Studeman, Subdirector da CIA e ex-director da NSA, 1 de Dezembro de 1992, McLean, Virgínia.
[86]Por exemplo, *Via Voice* da IBM, *Naturally Speaking* da Dragon, *Voice Xpress* da Lemout e Hauspe.
[87]"A Hidden Markov Model based keyword recognition system", R. C. Rose e D. B. Paul, *Proceedings of the International Conference on Accoustics, Speech and Signal processing* (actas da conferência internacional sobre acústica, fala e processamento de sinais), Abril de 1990.
[88]Centre de Recherche Informatique de Montreal (Centro de Investigação Informática de Montreal).
[89]"Project detection des Themes", CRIM, 1997; publicado em http://www.crim.ca/adi/projet2.html.
[90]Comunicação privada.
[91]NSA/CSS Classification Guide, NSA, revisto a 1 de Abril de 1983.
[92]"Rigging the game: Spy Sting", Tom Bowman, Scott Shane, *Baltimore Sun*, 10 de Dezembro de 1995.
[93]"Wer ist der Befugte Vierte?", *Der Spiegel*, **36**, 1996, p. 206-7.
[94]"Secret Swedish E-Mail Can Be Read by the U.S.A.", Fredrik Laurin, Calle Froste, *Svenska Dagbladet*, 18 de Novembro de 1997.