SIGA 2006

Auditório Pedro Calmon

Segurança e Tecnologia da Informação

13/Set/2006

Comandante Paulo Pagliusi

Assessor de Segurança da Informação

pagliusi@casnav.mar.mil.br

Marinha do Brasil

Amazônia Azul

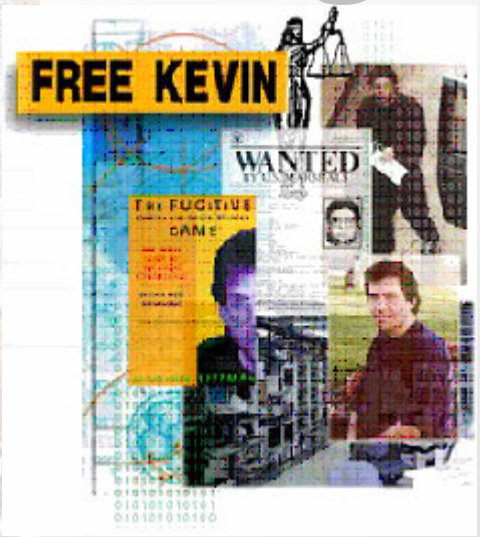
Tecnologia da Segurança de Informação

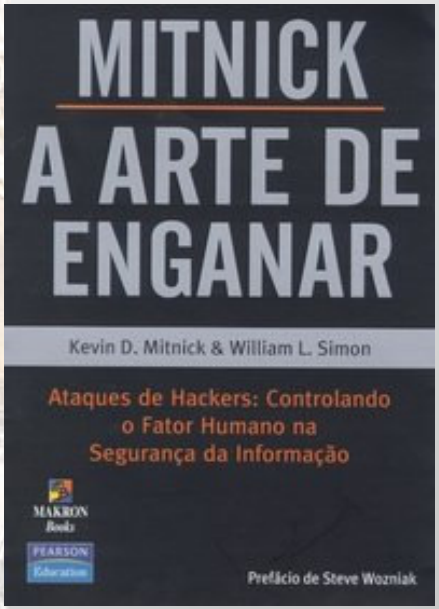
Métodos, técnicas e equipamentos empregados

Tecnologia da Guerra de Informação

- Engenharia Social
- Criptografia/Criptoanálise
- Monitoramento Eletrônico
- Tempest
- Softwares Maliciosos e Chipping
- Hacking

Engenharia Social





Técnica que um dos mais famosos hackers do mundo, Kevin Mitnick, fazia intenso uso.

http://www.kevinmitnick.com/

Autor: Kevin D. Mitnick, William L. Simon
Publicação: 2003
Editora: Makron Books

CASNAV

Engenharia Social

Simplesmente Pedindo...e Explorando a Vaidade Alheia...

Engenharia Social

Simplesmente Pedindo (2)... e Apagando os Vestígios...

Criptografia ???

Criptoanálise

2a. Guerra: Enigma e Bletchley Park

Criptoanálise

O Brasil como alvo

Livros como "The Codebreakers" de D. Kahn e "The Puzzle Palace" de J. Bamfort citam que os EUA quebraram códigos criptográficos brasileiros durante 1ª e 2ª GM.

NR 1595 CBKI57 5364A 19431021 BRAZIL/GENERAL COMMUNICATIONS DATA
NR 1595 CBKI57 5364A 19431021 BRAZIL/GENERAL COMMUNICATIONS DATA
NR 1606 CBKI62 5920A 19421023 SPANISH SHIPS AND CORRESPONDING NUMBERS USED BY BRAZILIAN
NR 1609 CBKI62 5939A 19431005 BRAZILIAN MESSAGE COMMUNICATIONS, CODES FOR SHIP REPORTING
NR 1939 CBLJ43 238A 19430712 PANAIR DO BRAZIL RADIO STATIONS IN AMAZON VALLEY
NR 2393 CBLM11 403A 19430223 GERMAN GOVERNMENT TELEGRAMS TO OR FROM BRAZIL IN SPANISH GOVERNMENT CODES
NR 3923 ZEMA123 46340A 19390000 BRAZILIAN DIPLOMATIC & CONSULAR CODE BOOKD - 1939
NR 3987 ZEMA138 45620A 19441207 CODES AND CIPHERS: BRAZIL BZD/BLDA BZC/BLDF
NR 3988 ZEMA138 45622A 19440000 CODES AND CIPHERS: BRAZIL BZA/BLDA-1 BZD/BLDA.
NR 4309 ZEMA180 36533A 19450129 CRYPTOGRAPHIC CODES AND CIPHERS: BRAZIL, SIS, SSA, BZ, CODES
NR 4310 ZEMA180 36534A 19170000 CRYPTOGRAPHIC CODES AND CIPHERS: BRAZIL, PORTUGUESE-BRAZILIAN MATERIAL IN FILES OF MI-8
NR 4678 ZEMA44 224A 19430913 COMPLETE DATA ON RADIO STATIONS OF THE BRAZILIAN MINISTRY OF AERONAUTICS
NR 4679 ZEMA44 289A 19400000 RECONSTRUCTED "OLD BRAZILIAN LETTER CODE"
NR 4687 ZEMA44 4848A 19400700 CODING INSTRUCTIONS FOR BRAZILIAN MILITARY ATTACHE


Monitoramento
Eletrônico
Rede Echelon

Quem coordena o Echelon ?

In God we trust

All others we monitor

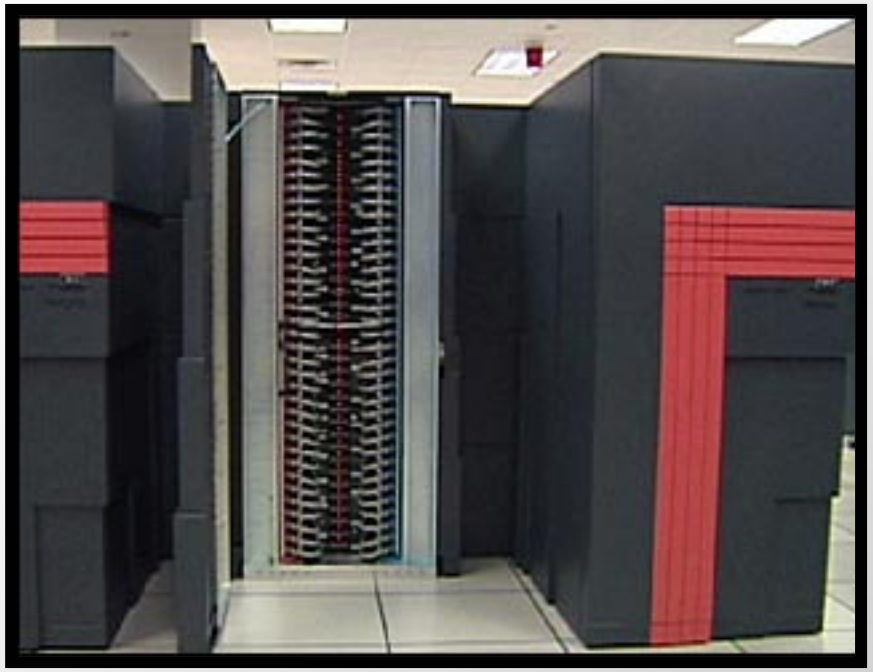
Quem é a NSA ?

Crypto City

Vista Aérea

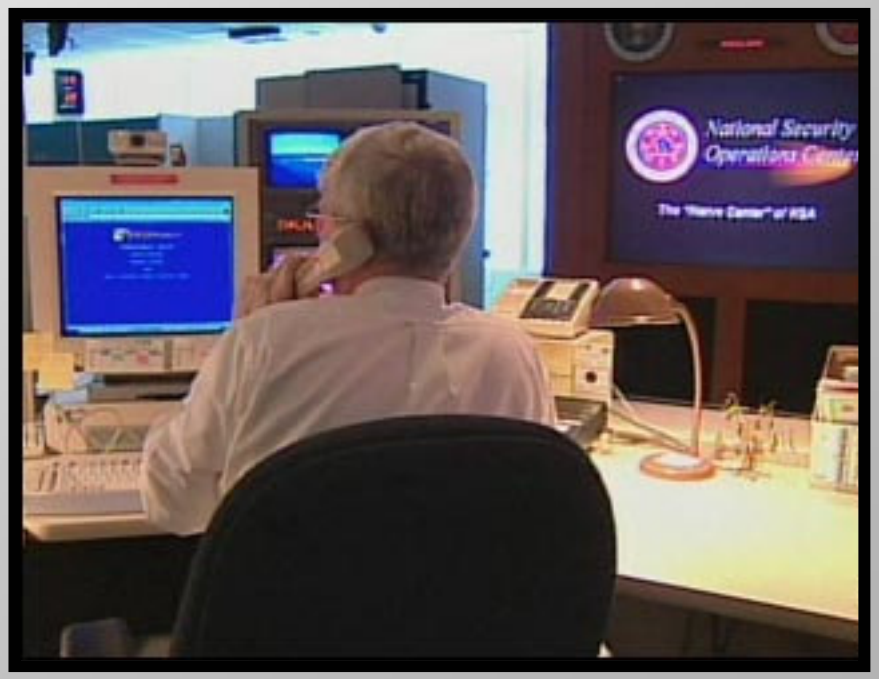
Centro de Comando de Emergência

Quem é a NSA ?



Supercomputador Cray

Interior da Agência



Os Parceiros

Nova Zelândia

GCSB

Inglaterra

GCHQ

EUA

NSA

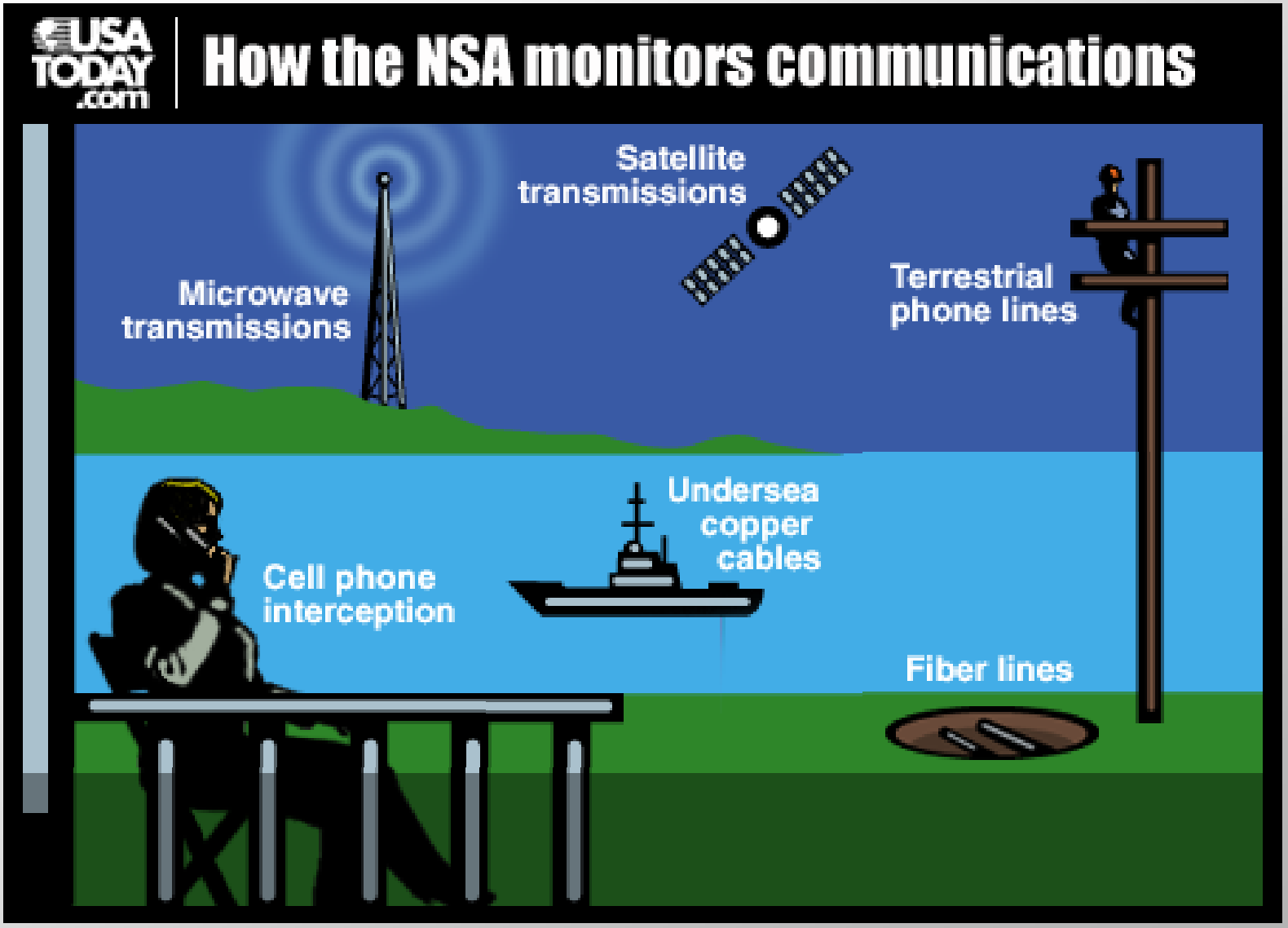
Canadá

CSE

Austrália

DSD

Como o Echelon monitora?



Quais os alvos do Echelon ?

Pós Guerra Fria - Área econômica e de desenvolvimento científico e tecnológico

Recentes - Narcotráfico lavagem de dinheiro terrorismo e crime organizado

Tradicionais - Comunicações militares e diplomáticas da ex-URSS

O que a NSA monitora?

Chamadas telefônicas e de fax, transmissões de rádio, Internet e telex em todo o mundo.

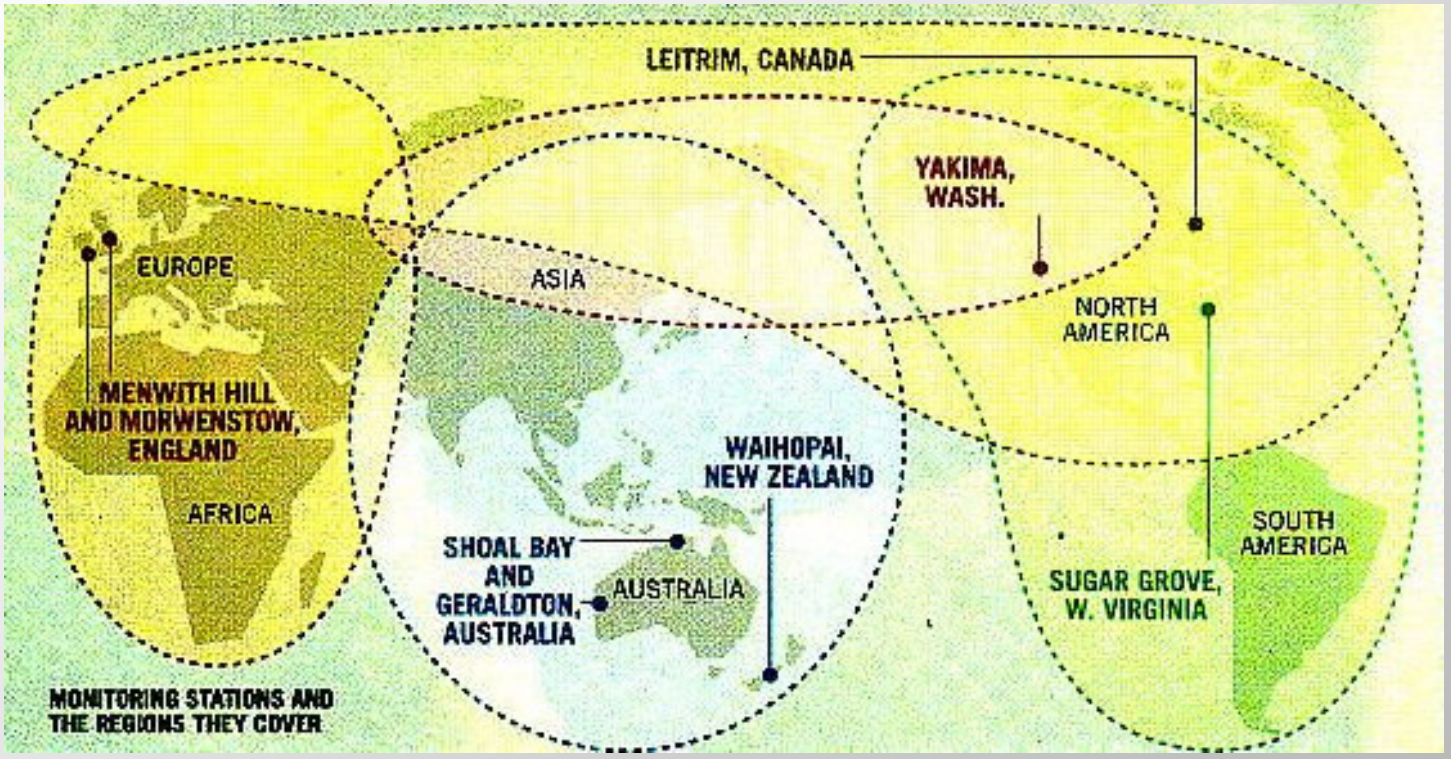
O que a NSA monitora?

Chamadas telefônicas e de fax, transmissões de rádio, Internet e telex em todo o mundo.

O que a NSA monitora?

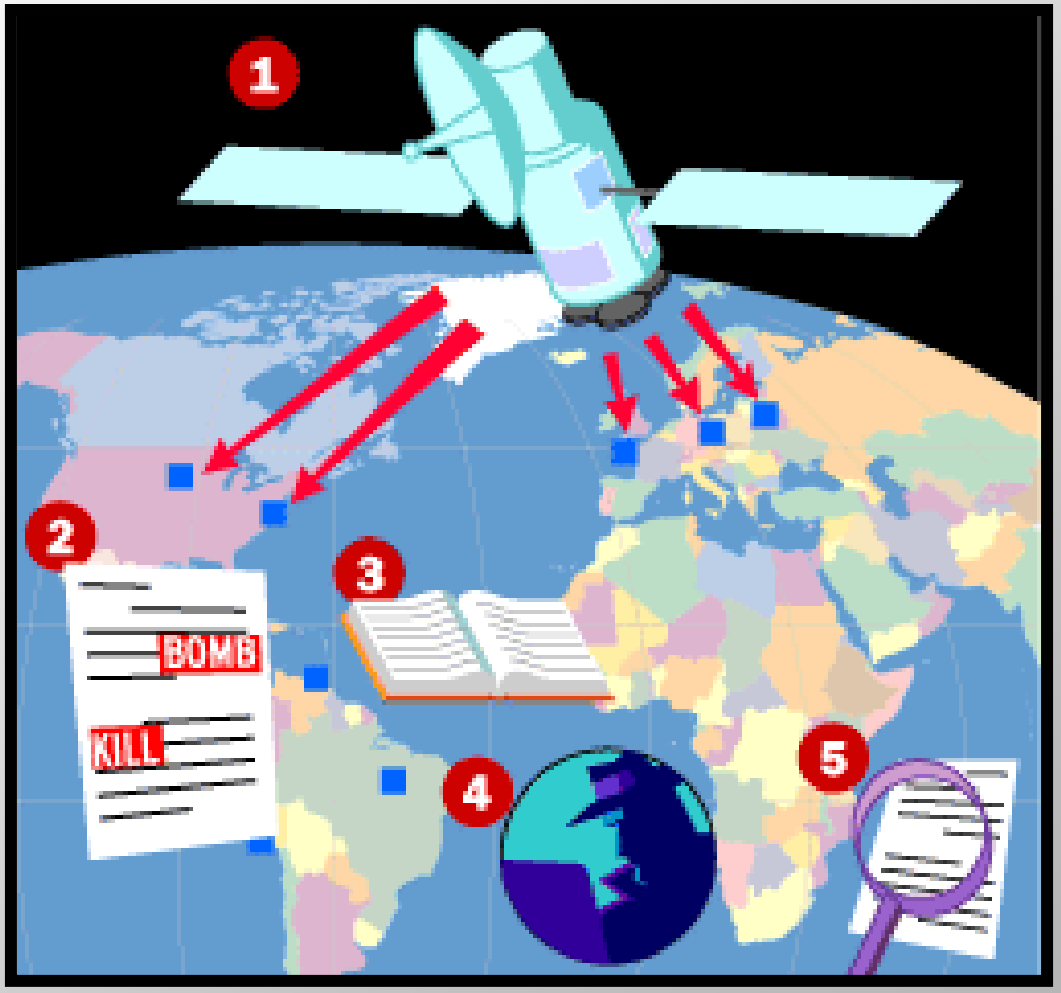
Chamadas telefônicas e de fax, transmissões de rádio, Internet e telex em todo o mundo.

O que a NSA monitora?



Chamadas telefônicas e de fax, transmissões de rádio, Internet e telex em todo o mundo.

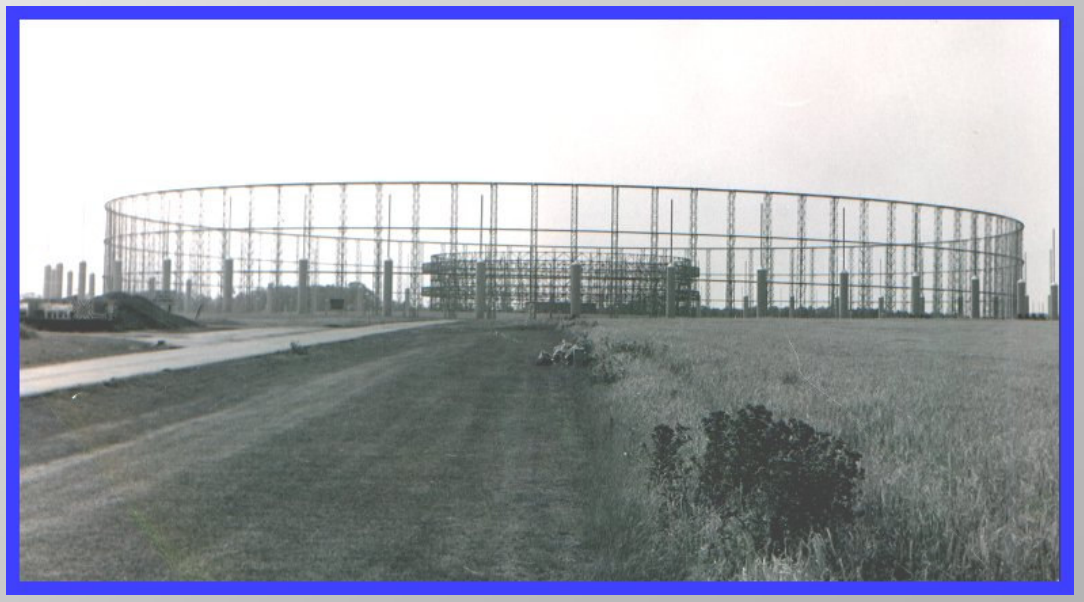
Como funciona o Echelon ?



Tipos de interceptação

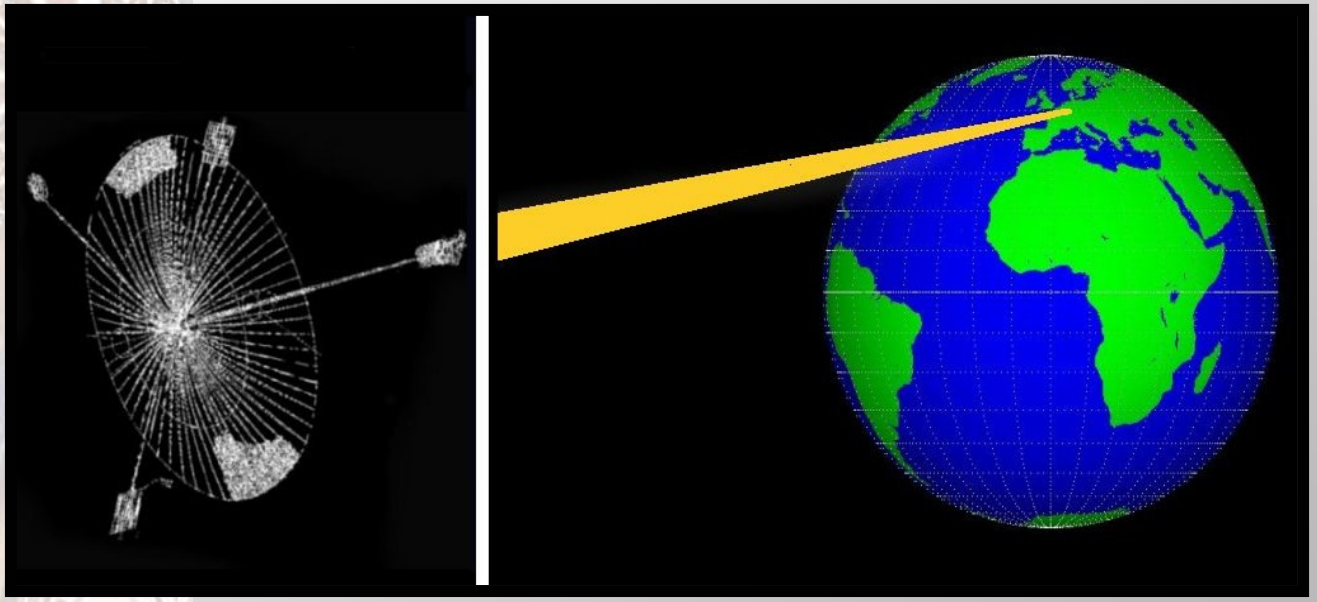
Comunicações em HF - Um dos principais meios para prover comunicações internacionais até 1960. Sua interceptação era rotineira e relativamente fácil.

Sistema AN/FLR-9
Instalado em bases na Inglaterra, Escócia, Itália e Turquia.



Tipos de interceptação

Comunicações por microondas - Exigem várias estações retransmissoras ao longo do percurso.

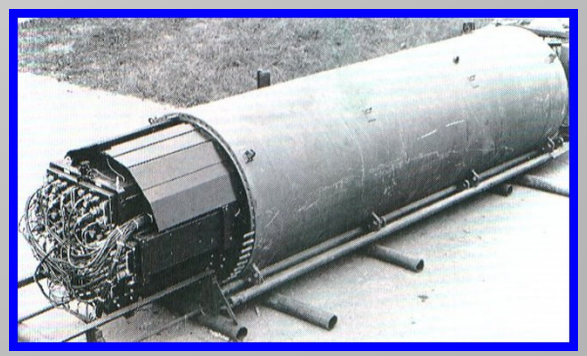


Tipos de interceptação

Comunicações por cabos submarinos - Aparentemente o mais seguro dos meios de comunicação. A interceptação seria possível apenas nas bases terrestres, onde os cabos retornam à superfície.

No entanto, em 1971, o USS Halibut visitou o Mar de Okhotsk, na costa da ex-URSS, e gravou comunicações que passavam por um cabo submarino soviético.

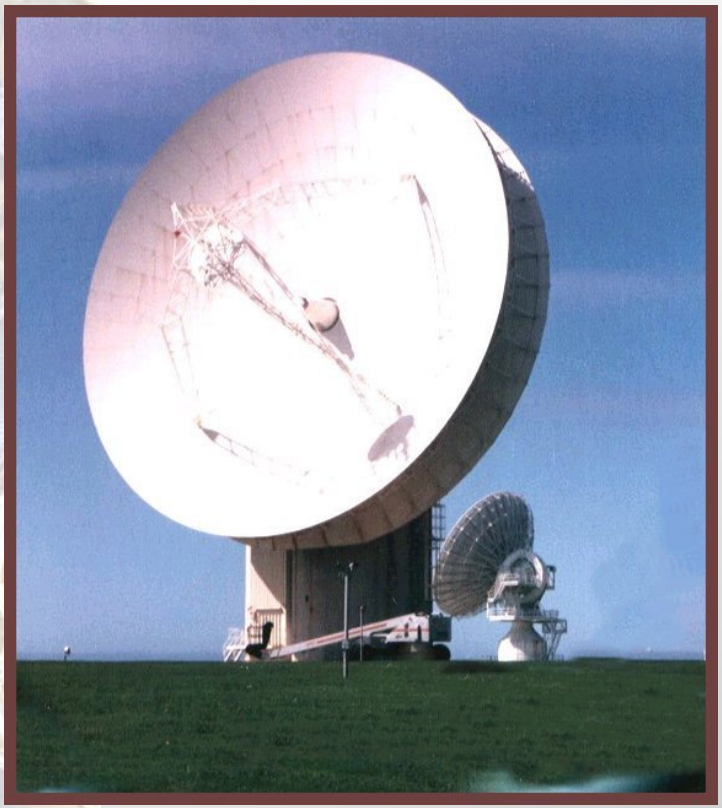
A gravação era efetuada por um **casulo** que era lançado pelo submarino e grampeado no cabo por mergulhadores. Rotineiramente, o submarino retornava ao local para recolher o casulo antigo e depositar novos.



Tipos de interceptação

Comunicações por Satélites - A interceptação dos satélites de comunicações internacionais iniciou-se por volta de 1971.
Sendo satélites geoestacionários com órbita próxima ao Equador, estes satélites são monitorados por estações terrenas localizadas em bases pertencentes às nações que compõem a aliança UK USA.

Estação de Monitoramento de Pine Gap, Austrália



Antena de 30m, em Morwenston, Inglaterra, interceptando comunicações de satélites regionais localizados nos Oceanos Atlântico e Índico.

Conjunto de antenas em Sugar Grove, EUA, direcionadas à satélites de comunicações regionais localizados na Europa e no Oceano Atlântico (Brasil).

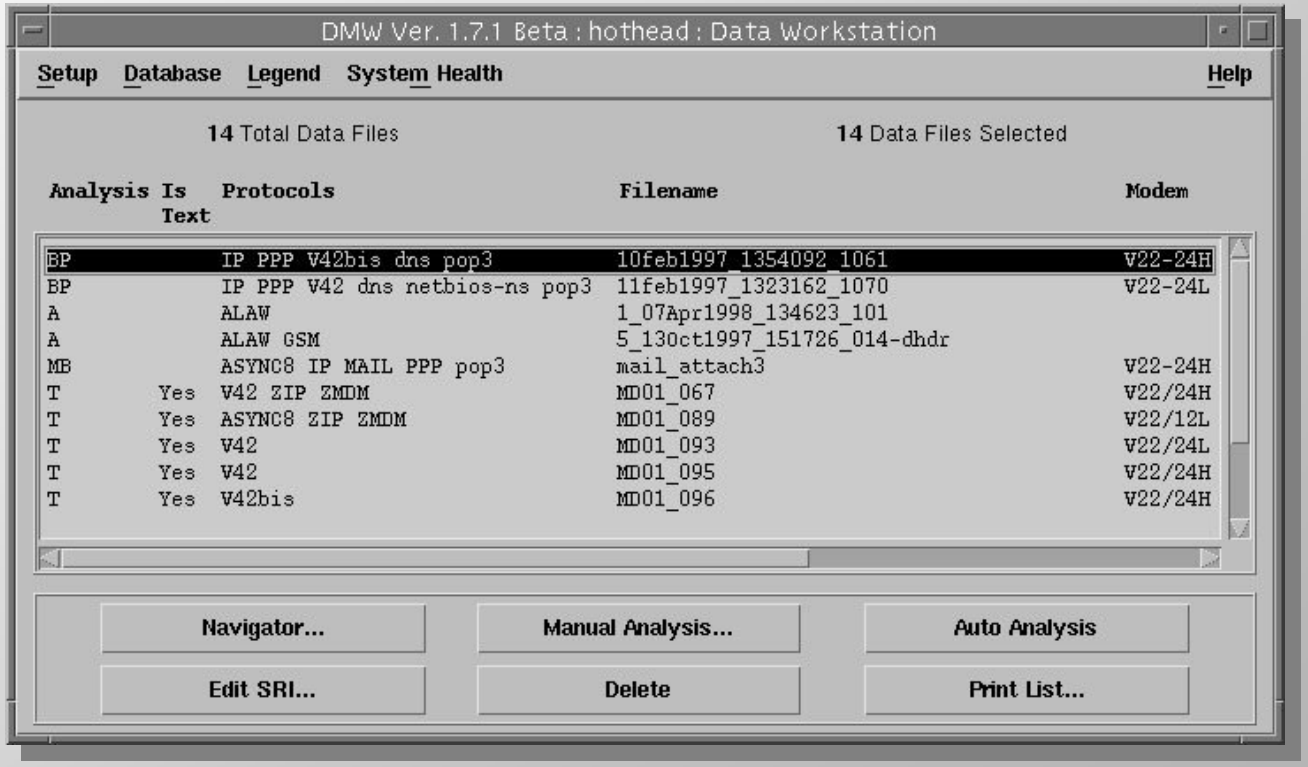
Estação de Monitoramento de Menwith Hill, Inglaterra

Estação de Monitoramento de Leitrim, Canadá

Menwith Hill

Tipos de interceptação

Comunicações pela INTERNET - O programa de Inteligência de Comunicação "Data Workstation" armazena e processa automaticamente 10.000 sinais distintos gravados, identificando o tráfego na Internet, *e-mails e attachments (Data mining e text mining)*.



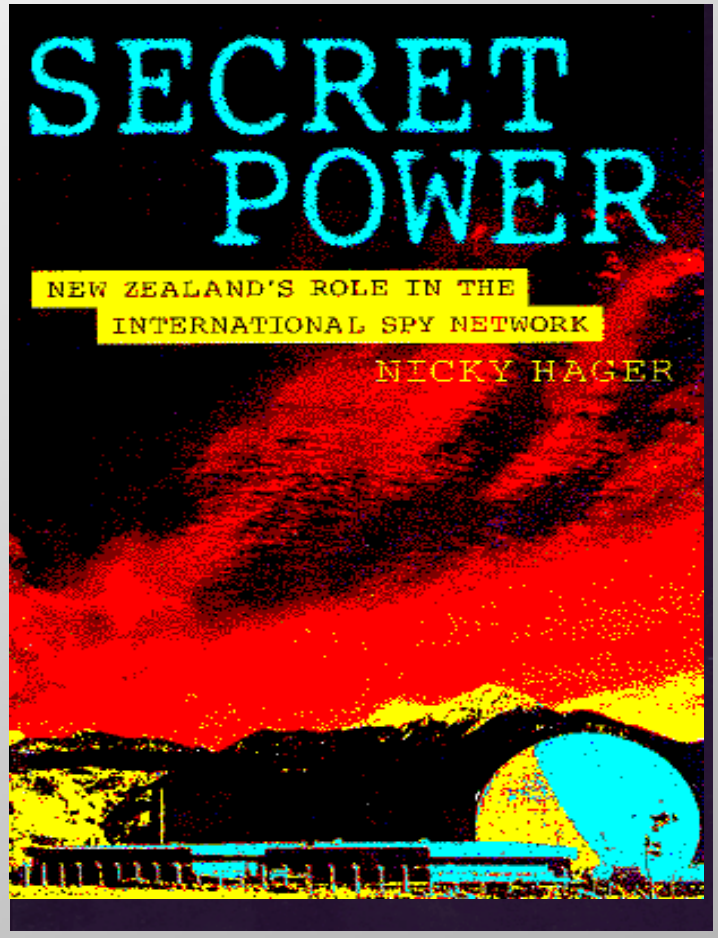
E a notícia do Echelon chega ao Brasil ...

Mais do que evidências ...

"The Puzzle Palace"
James Bamford, 1982

"Somebody's listening"
Duncan Campbell, 1988

"Secret Power"
Nick Hager, 1996



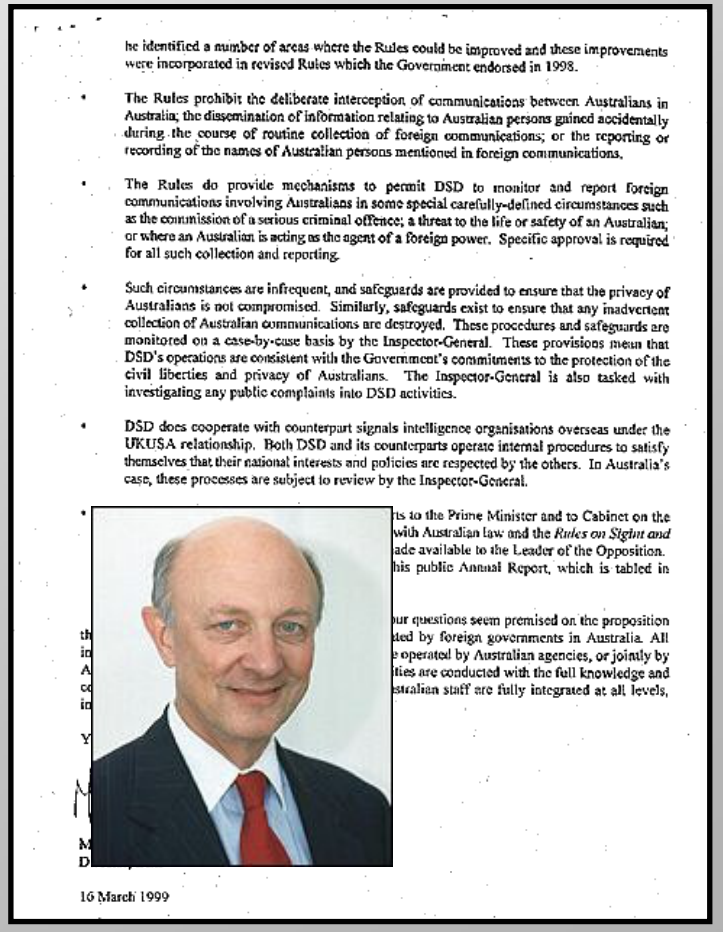
"An appraisal of the Technologies of Political Control"
Relatório do STOA ao Parlamento Europeu, 1998

Mais do que evidências ...

"Development of Surveillance Technology and Risk of Abuse of Economic Information"
Relatório do STOA ao Parlamento Europeu, 1999

Entrevista de Martin Brady,
Diretor do DSD (Aus), em 23/05/1999

Entrevista de James Woolsey,
ex-Diretor do CIA em 07/03/2000



he identified a number of areas where the Rules could be improved and these improvements were incorporated in revised Rules which the Government endorsed in 1998.

- The Rules prohibit the deliberate interception of communications between Australians in Australia; the dissemination of information relating to Australian persons gained accidentally during the course of routine collection of foreign communications; or the reporting or recording of the names of Australian persons mentioned in foreign communications.

- The Rules do provide mechanisms to permit DSD to monitor and report foreign communications involving Australians in some special carefully-defined circumstances such as the commission of a serious criminal offence; a threat to the life or safety of an Australian; or where an Australian is acting as the agent of a foreign power. Specific approval is required for all such collection and reporting.

- Such circumstances are infrequent, and safeguards are provided to ensure that the privacy of Australians is not compromised. Similarly, safeguards exist to ensure that any inadvertent collection of Australian communications are destroyed. These procedures and safeguards are monitored on a case-by-case basis by the Inspector-General. These provisions mean that DSD's operations are consistent with the Government's commitments to the protection of the civil liberties and privacy of Australians. The Inspector-General is also tasked with investigating any public complaints into DSD activities.

- DSD does cooperate with counterpart signals intelligence organisations overseas under the UKUSA relationship. Both DSD and its counterparts operate internal procedures to satisfy themselves that their national interests and policies are respected by the others. In Australia's case, these processes are subject to review by the Inspector-General.

- ts to the Prime Minister and to Cabinet on the with Australian law and the *Rules on Sigint and* ade available to the Leader of the Opposition. his public Annual Report, which is tabled in

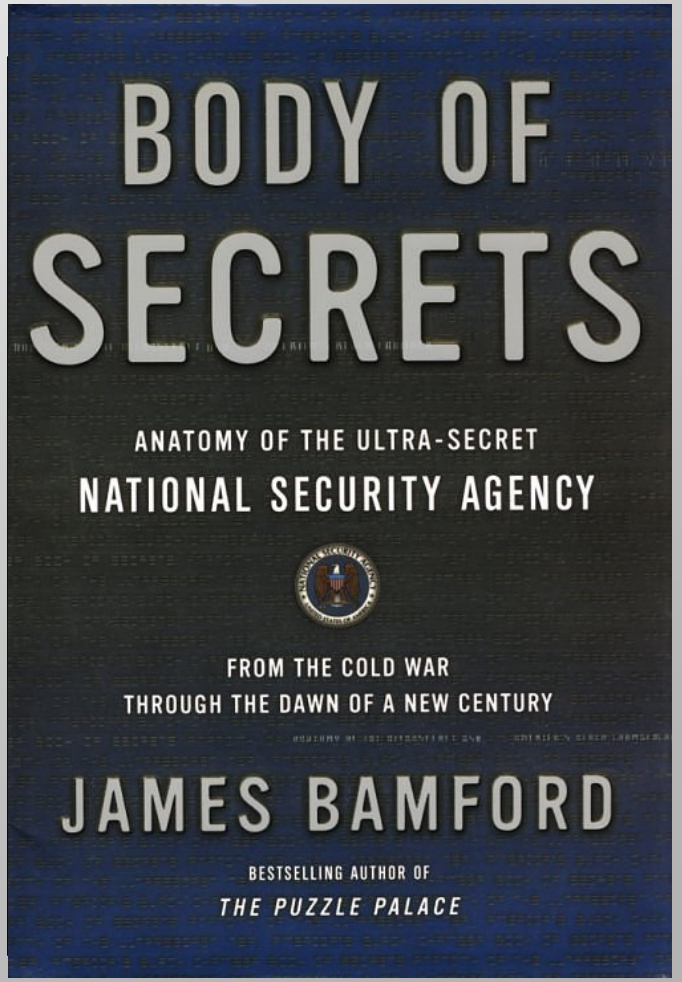
ur questions seem premised on the proposition ted by foreign governments in Australia. All operated by Australian agencies, or jointly by ties are conducted with the full knowledge and stralian staff are fully integrated at all levels,

16 March 1999

Mais do que evidências ...

"Body of Secrets"
James Bamford, 2001

"Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)"
Relatório de Gerhard Schmid ao Parlamento Europeu, 2001



E o Parlamento Europeu?

Divulgação dos Relatórios do STOA ao Parlamento Europeu causa mal-estar entre os países membros:

Europeus receosos de acusarem EUA por algo que não é admitido oficialmente.

Alguns países possuem tratados bilaterais com os EUA.

Alguns países possuem interesses próprios nesta área.

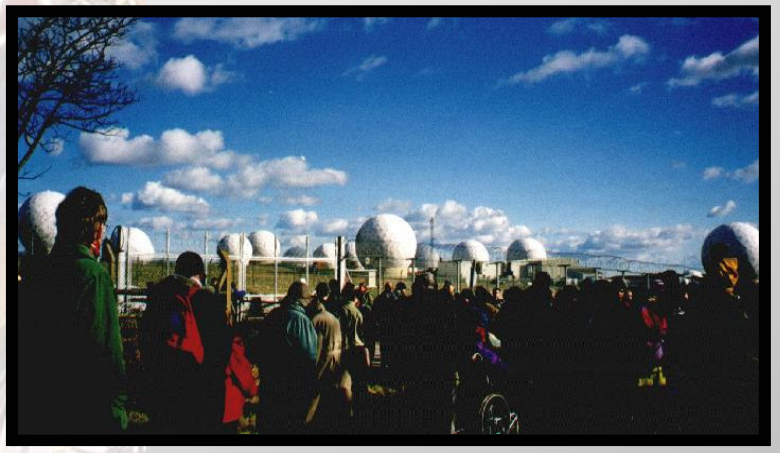
Grupos de Ativistas

Campanha para o fechamento de Menwith Hill

MENWITH HILL U.S. SPY STATION

Nr. Harrogate, North Yorkshire, England

- It's the most secret U.S. Base In Britain ....
- It's the world's largest spy base ....
- It's unaccountable .... and it's getting bigger ....



O que pode atrapalhar o Echelon ?

O uso generalizado de criptografia

O uso de criptografia forte

A resposta dos EUA ...

EUA restringe exportação de software e hardware criptográficos

Exportação de *hardware* e *software* criptográfico equiparada à de armamento (Munitions Control Act).

Tratado de Wassenaar restringe a exportação de:

- sistemas simétricos até 56 bits;
- sistemas assimétricos até 512 bits.

Tratamento especial:

- bancos e empresas que efetuam transações monetárias.

Nova política de exportação

A Casa Branca divulgou em 2000 novas regras de controle para exportação de software e hardware criptográficos.

A indústria pode exportar produtos criptográficos com chaves de qualquer tamanho sem necessidade de licença. Mas deve submetê-los a uma "inspeção técnica" prévia do Departamento de Comércio norte-americano.

Permanece a barreira para os 6 países considerados pelo EUA Estados terroristas: Coréia do Norte, Cuba, Irã, Iraque, Síria e Sudão.

Efeito TEMPEST ???

Obtenção de informações oriundas das emanações eletromagnéticas secundárias irradiadas pelos computadores:

- Transientes
- Provocadas

Monitor de emissões TEMPEST DataSafe/ESL 400 (década de 80)

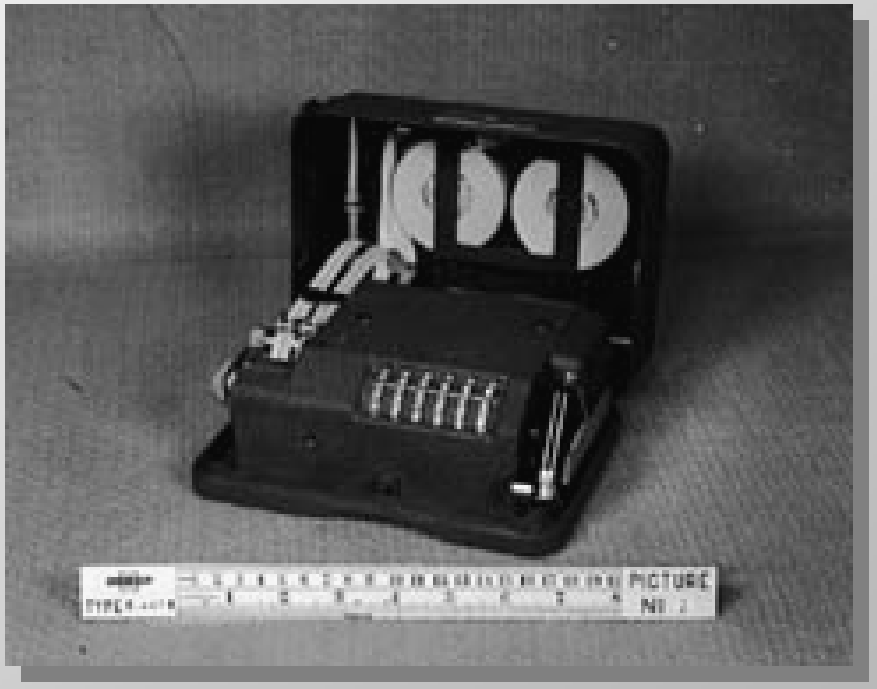
Caso CRYPTO AG

A CRYPTO AG é uma empresa suíça que desde a 2ª Guerra forneceu equipamentos criptográficos para mais de 130 países, valendo-se da imagem de neutralidade de seu país.

Caso CRYPTO AG

Graças a um possível relacionamento CRYPTO AG - NSA, durante décadas os EUA teriam interceptado e decifrado mensagens sigilosas cifradas de dezenas de países.

Estas nações haviam adquirido da CRYPTO AG a mais sofisticada e supostamente segura tecnologia de criptografia comercial disponível.



Entretanto, os equipamentos da CRYPTO AG transmitiriam, automática e clandestinamente, as chaves criptográficas utilizadas junto com as mensagens cifradas.

Caso CRYPTO AG

O manto acobertando o relacionamento NSA-Crypto AG se desfez em Mar/92, quando o serviço de contra-inteligência militar iraniano seqüestrou Hans Buehler, representante comercial da Crypto AG em Teerã.

Depois do seqüestro, a imagem de neutralidade da Crypto AG foi arranhada e várias nações reexaminaram seus acordos de segurança.

Caso chave NSA do Windows

Pesquisando sobre a arquitetura CryptoAPI da Microsoft, Andrew Fernandes, cientista-Chefe da Cryptonym, denunciou que em toda cópia do Win95/98/NT4 e Windows2000 teria instalada uma "back door" para a NSA.

Fonte: Cryptonym, 31/08/99.

Caso PSN no Pentium III

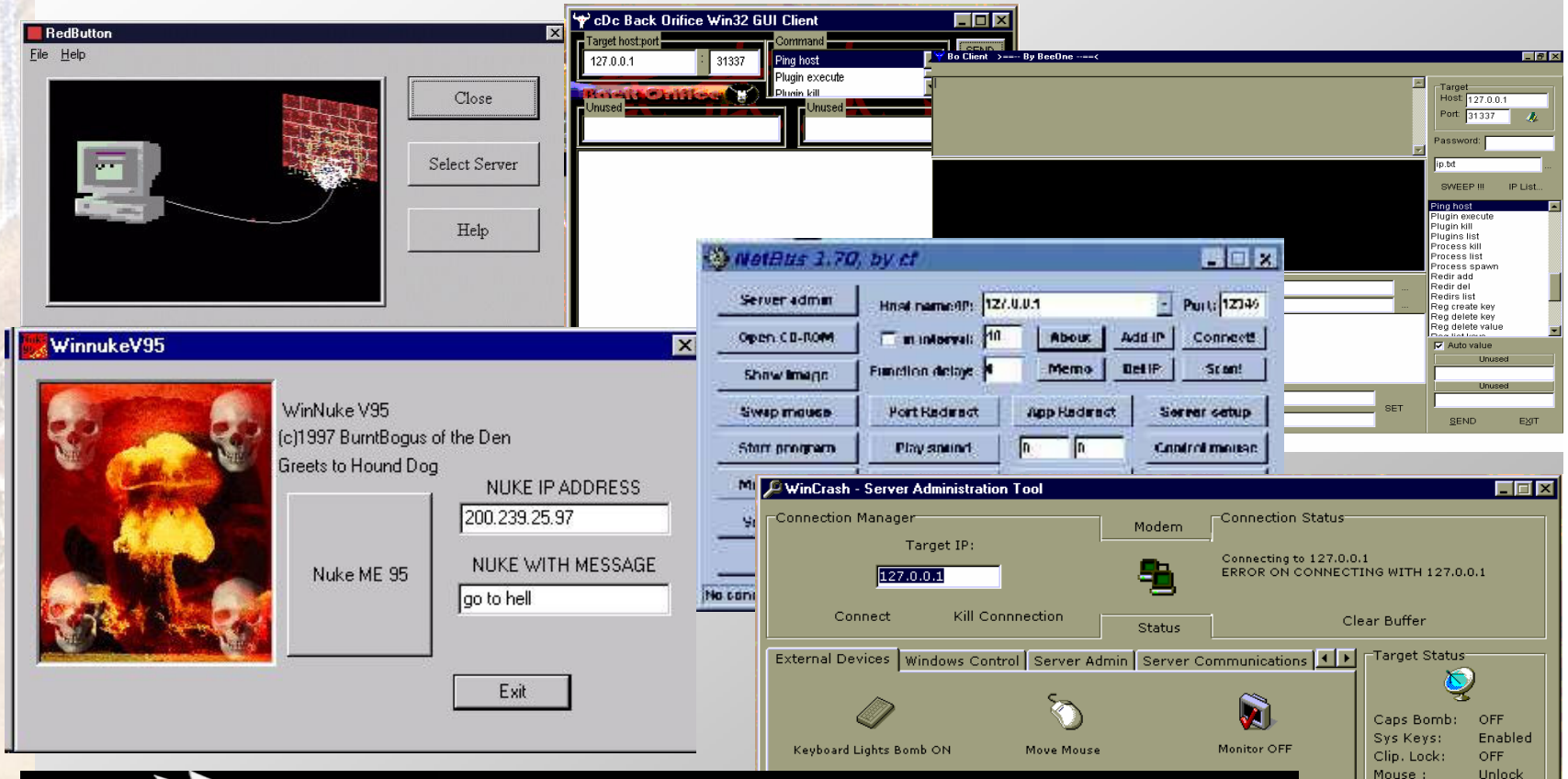
Hacking

Ataques a Web Sites

- Roubo de dados de cartões de crédito
- DDOS (*Distributed Denial of Service*)
- Modificação de Páginas

Fonte: Secunet

Ferramentas de Ataque



LØPHT HEAVY INDUSTRIES

It's big. It's Bad. It cuts throug NT Passwords like a diamond tipped, steel blade. It ferrets them out the registry, from the repair disks, and by sniffing the net like an anteater on dexadrene

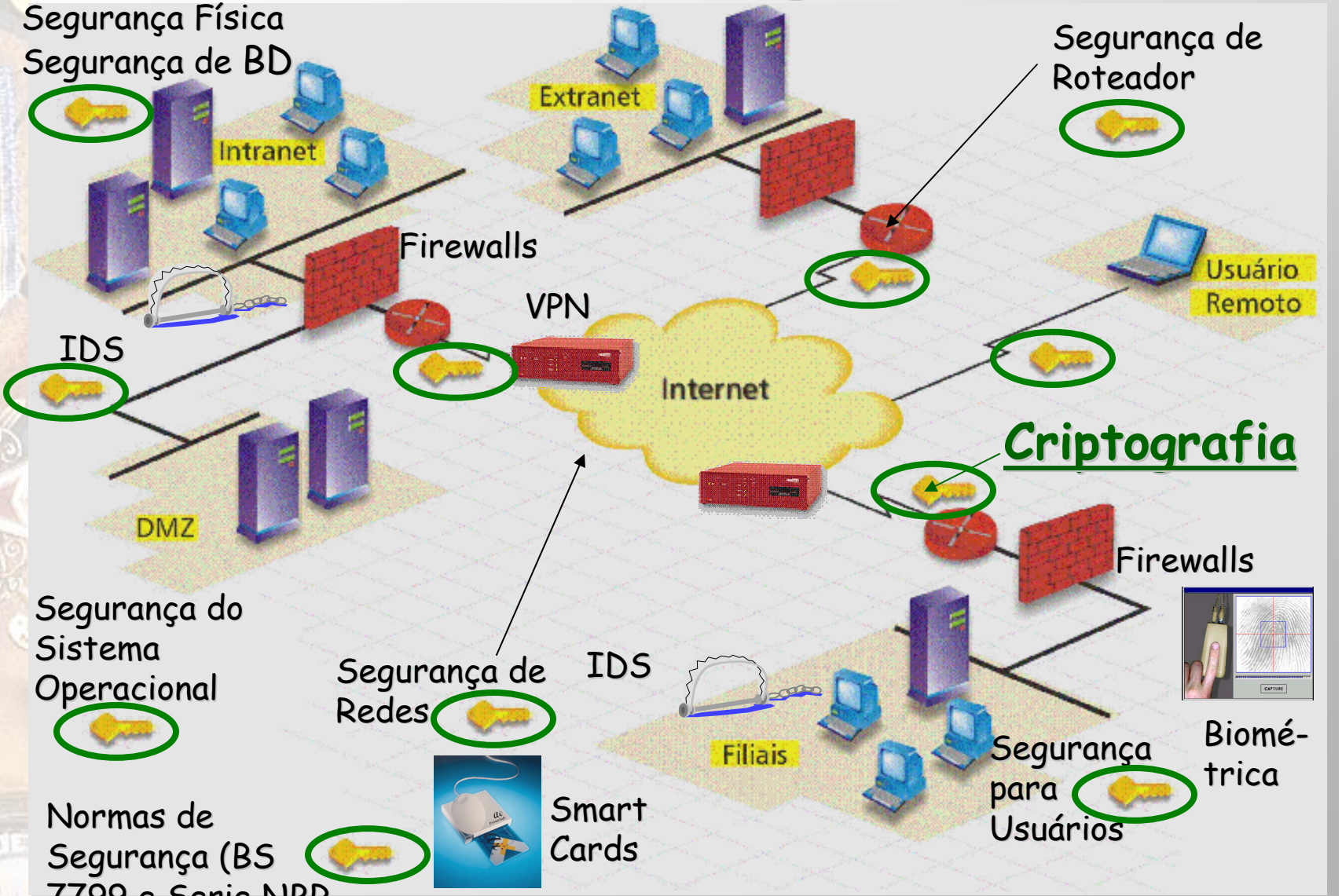
Procedimento Completo de Um Ataque

- Achar sistema vítima
- Identificar vulnerabilidade no sistema vítima
- Conseguir acesso não autorizado
- Atividade maliciosa
- Tirar benefício da atividade
- Deletar todos os rastros

Contramedidas de Segurança da Informação

PSI, firewalls, VPN, IDS, biométrica, smartcards, Criptografia.

Modelo de Segurança



Programa de Segurança da Informação: Evolução

Como está a Política de Segurança da Informação da sua organização?

Fonte: Módulo - F. Nery.

Segurança da Informação

IPLAN – Teatro do Grupo de Segurança

Segurança de Usuários
Cuidados Especiais

- *E-mail*
  - Vírus,
  - *Mail Bombs*,
  - Cavalos de Tróia.
- Vazamento de Informações
  - Engenharia Social.
- Navegadores (executa sem prompt, com prompt, não executa)
  - *Java VM, JavaScript, ActiveX, cookies*.
- Administração segura do acesso de servidores e contratados
  - máquinas, diretórios, arquivos e horários.
- Senhas
  - Sigilo, troca freqüente e cuidados na construção.

O Que São Senhas Fracas

- Dados biográficos ou outros que possam ser associados ao usuário.
- Palavras de dicionários (de qualquer língua).
- Somente números.
- Somente letras.
- Senhas pequenas (< 8 caracteres).

Como criar Senhas Fortes?

- Mistura de letras maiúsculas com minúsculas.
  aydTkaMfuyGbnWd
- Números e caracteres especiais.
  - @25742${?$#&!98, smiles :) = ☺ :[:{0
- Palavras ou frases grafadas de forma errônea (memorização).
  - esplicassam, meinerva, xcudo
- palavras ou frases grafadas sem as vogais ou somente as iniciais de frases.
  - minha geladeira azul = mnhgldrzl ou mga
- O ideal é misturar tudo.
  - @2004:)MnhGldrZl

Referências

Livros:

Zuffo, Joâo Antônio, " A Infoera - O Imenso Desafio do Futuro, Ed. Saber, 1997.

Libicki, Martin, " What is Information Warfare ?", ACT, 1995.

McClure, S. et all, "Hackers Expostos", Makron Books, 2000.

Sun Tzu - A Arte da Guerra. Tradução, introdução e Notas, Cultura Editores Associados, 1994.

Períodicos:

AFCES´s International Journal, January 2002.

Referências (continuação)

Sites:

BBC

http://news.bbc.co.uk

IW e relacionados com contra-medidas de segurança

- www.infowar.com
- www.sbccom.army.mil
- www.nipc.gov
- www.fedcirc.gov
- www.cert.org
- www.nsa.gov
- www.infocentre.ru
- www.chechnya.ru
- www.web.amnesty.org

Referências (continuação)

Tecnologias de Ataque e de Contra-Inteligência:

- RSA Labs FAQ
  - http://www.rsa.com/rsalabs/faq/index.html (HTML)
- Advanced Encryption Standard (AES)
  - http://www.nist.gov/aes/
- Legislação Mundial sobre Criptografia
  - http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
- Chave espiã da NSA no Windows.
  - http://www.cryptonym.com/hottopics/msft-nsa.html
- Peter Gutman's Encryption & Security.
  - http://www.cs.auckland.ac.nz/~pgut001/links.html
- Revista Wired News.
  - http://www.wired.com/news/news/technology/story/22102.html

Echelon

- Filme Echelon
- Parlamento Europeu (Echelon/Crypto AG)
  - http://www.europarl.eu.int/dg4/stoa/en/

Marinha do Brasil

www.mar.mil.br

Perguntas?

Marinha do Brasil
Centro de Análises
de Sistemas Navais

Comandante Paulo Pagliusi

Assessor de Segurança da Informação
pagliusi@casnav.mar.mil.br
Tel. (21) 2178-6925.