IndianZ

Espionage

Espionage means to obtain classified information without permission.

December 2010

Agenda

- Einführung
- Bedrohung
- Wirtschaftskrieg
- Informationen
- Spionagetechnik
- Alarm Signale
- Abwehrtechnik

Einführung

- **Spionage ist die Auskundschaftung und Erlangung fremder Geheimnisse oder geschützten Wissens**
- **Sehr komplexes Gebiet, Technisch**
  - **Aktiv: Funk (1 kHz bis 110 GHz) und Kabel, Passiv: Aufnahmegeräte**
  - **Audio, Video, Daten**
- **Nicht technisch**
  - **Social Engineering, Online-Recherchen**
- **Günstige Beschaffung Spionageausrüstung**
- **Unter 1‘000 CHF für gute Abhörgeräte (unter 100 CHF)**
- **Wenig öffentliche Informationen, sehr hohe Dunkelziffer**

Einführung

- **Spezialisten kontaktieren**
  - **Kein internes/eigenes Telefon, kein internes Email**
  - **Münztelefon 5-10 km entfernt, neu gekauftes Mobiltelefon**
  - **Im Internet-Cafe neu eingerichtetes Email (gmx, hotmail, google)**
- **Nicht selbst die Wanzen zu finden versuchen**
- **Nicht im Büro, Auto, der Öffentlichkeit (mit anderen Anwesenden) oder zuhause davon reden**
- **Erstes Treffen in der Öffentlichkeit, dabei ALLE elektronische Geräte deaktivieren (nicht nur ausschalten, Batterie/Akku rausnehmen)**

Bedrohung

- Jegliche Produkte- und Preisinformationen
- Stock Trade (Börse)
- Finanzdienstleister, Banken
- Politische und/oder gerichtliche Aktivitäten
- Militär, Rüstung, Regierung, Strafverfolgung
- Raumfahrt, Mikroelektronik
- Marketing, Mode, Industrie, Werbung
- Pharma, Chemie, Gentechnik
- Racheakte, Whistle-Blowing

Bedrohung

- **Wirtschaftskriegsführung, seit Clinton-Ära pusht USA diesen Bereich**
- **Global Players:**
  - **USA, England, Australien, Neuseeland, Kanada, Israel, Frankreich, China, Japan**
  - **Frankreich hat Schule seit 2001**
    - **www.ege.fr**
  - **Beispiel 1994/95**
    - **ENERCON/Kenetech Windpower**
  - **Beispiel 2007**
    - **Formel 1**

COMINT/ELINT

- COMINT (Communication Intelligence)
  - Abhören Kommunikation (Leute)
  - Direkte Abhörmassnahmen
  - VHF/UHF
- ELINT (Electronic Intelligence)
  - Abhören Kommunikation (Maschinen)
  - Elektronische Sensoren
  - Identifizierung Maschinen

HUMINT/SIGINT

- **HUMINT (Human Intelligence)**
  - **„Social Engineering“**
  - **Gesprächsabschöpfung**
  - **Einschleusung (langfristig)**
  - **Anbahnung (Romeo-Masche)**
  - **Bestechung, Erpressung**

- **SIGINT (Signals Intelligence)**
  - **Abhören Kommunikation (COMINT/ELINT)**
  - **Auffangen sonstiger Funkübertragungen**

OSINT

- **OSINT (Open Source Intelligence)**
  - **Internet Recherchen, Websites**
  - **Google, Newsgroups, Social Networks**
  - **Messen, Veranstaltungen**
  - **Publikationen**
  - **Angebotsanforderungen**
  - **Joint Ventures/Übernahmen**
  - **Chat, Filesharing**
  - **Whois, DNS, Telefonbuch, Karten**

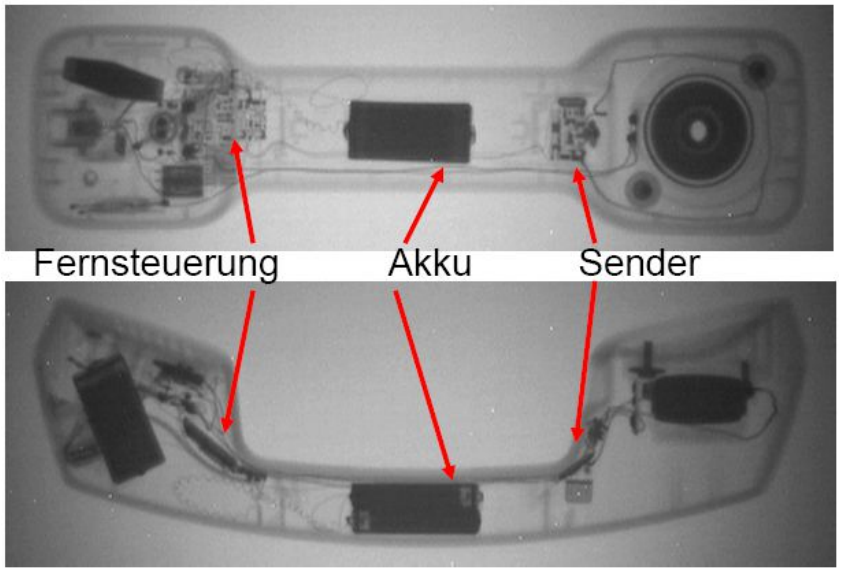
Technik

- Bugs (Wanzen)
  - Akustisch (Stethoskop)
  - Ultraschall VLF (über hörbarem Bereich)
  - Radiofrequenz RF (Funk)
  - Optisch (Laser)
  - Hybrid (Mischung obiger Typen)
- Wiretapping
  - Hardwired (am Kabel)
  - Soft (TVA-Software)
  - Record (Tape Recorder)
  - Transmit (RF)

Technik

- **Kommunikation**
  - **Lokales Abhören von Telefonanlagen**
  - **Abhören von Seekabeln und Richtfunkstrecken**
  - **Abhören der Kommunikationssatelliten**
  - **Auswertung durch Zielkontrolle und Hitwörter**
  - **Analyse von Kommunikationsprofilen**
- **Telefon**
  - **Was eine Antenne hat, ist nicht sicher!**
  - **Telefon, PBX, Beantworter, ISDN, FAX, Modem**

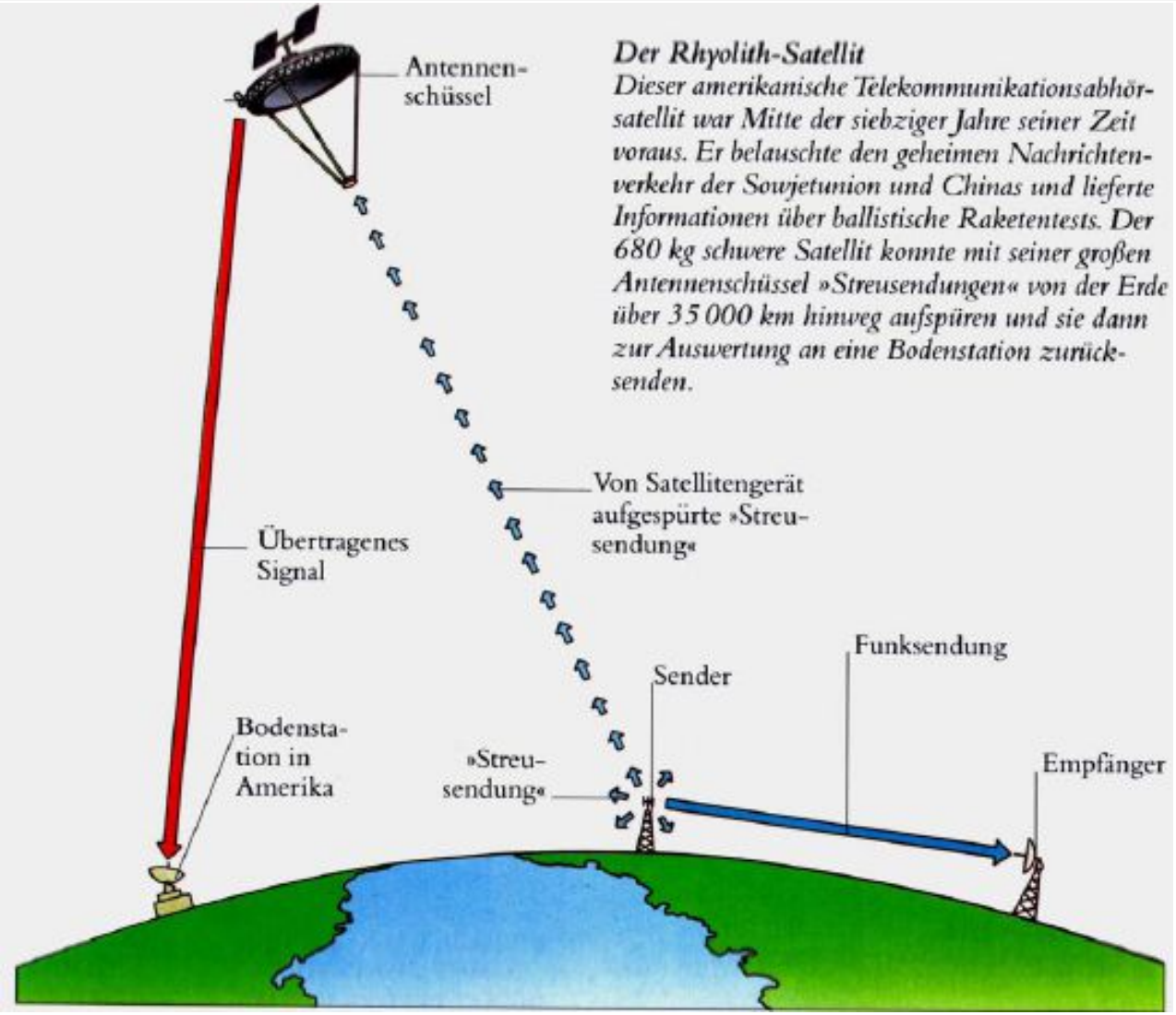
Technik



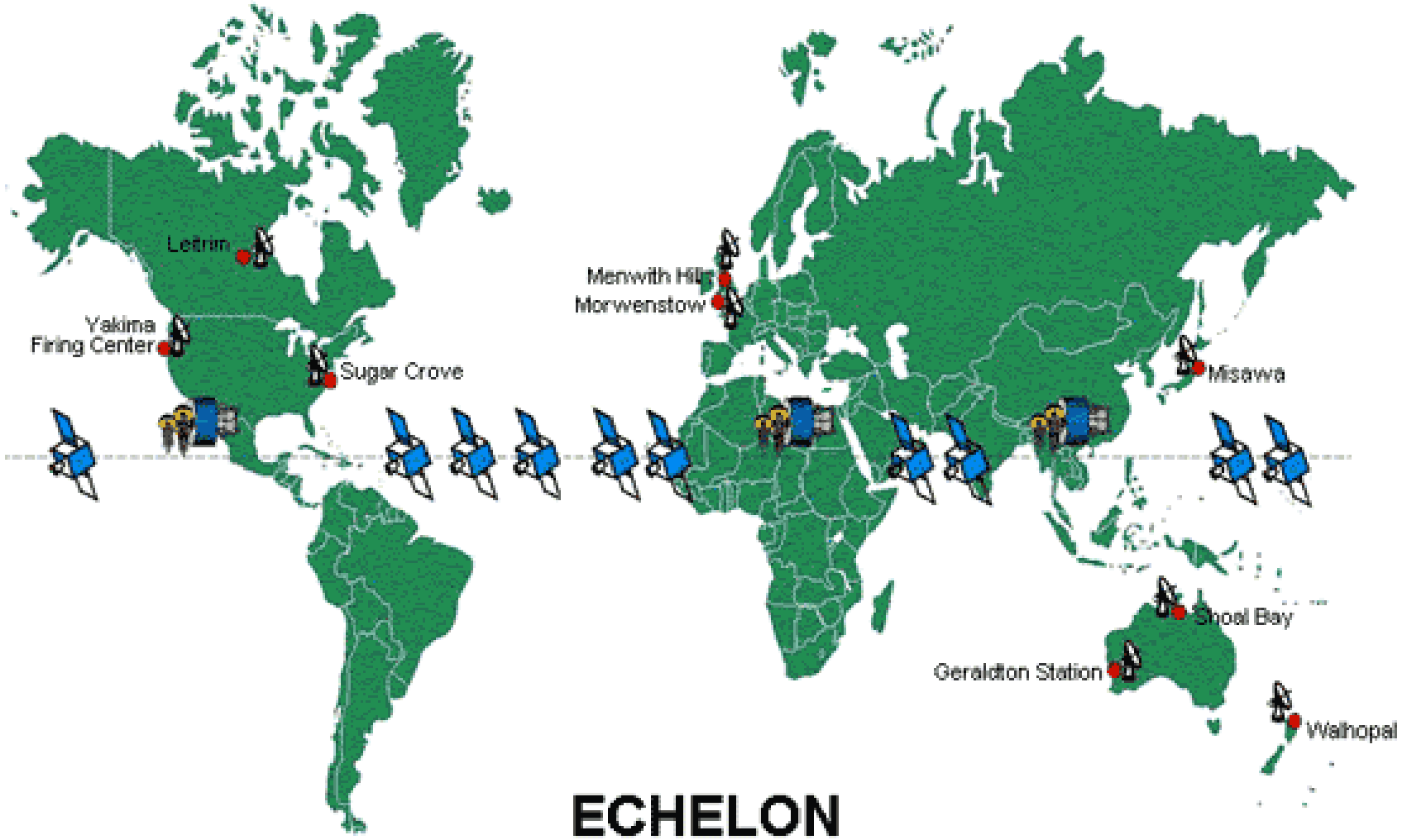
Technik

Technik

Technik


Antennen-
schüssel
Der Rhyolith-Satellit
Dieser amerikanische Telekommunikationsabhör-
satellit war Mitte der siebziger Jahre seiner Zeit
voraus. Er belauschte den geheimen Nachrichten-
verkehr der Sowjetunion und Chinas und lieferte
Informationen über ballistische Raketentests. Der
680 kg schwere Satellit konnte mit seiner großen
Antennenschüssel »Streusendungen« von der Erde
über 35 000 km hinweg aufspüren und sie dann
zur Auswertung an eine Bodenstation zurück-
senden.
Von Satellitengerät
aufgespürte »Streu-
sendung«
Übertragenes
Signal
Funksendung
Sender
Bodenstа-
tion in
Amerika
»Streu-
sendung«
Empfänger

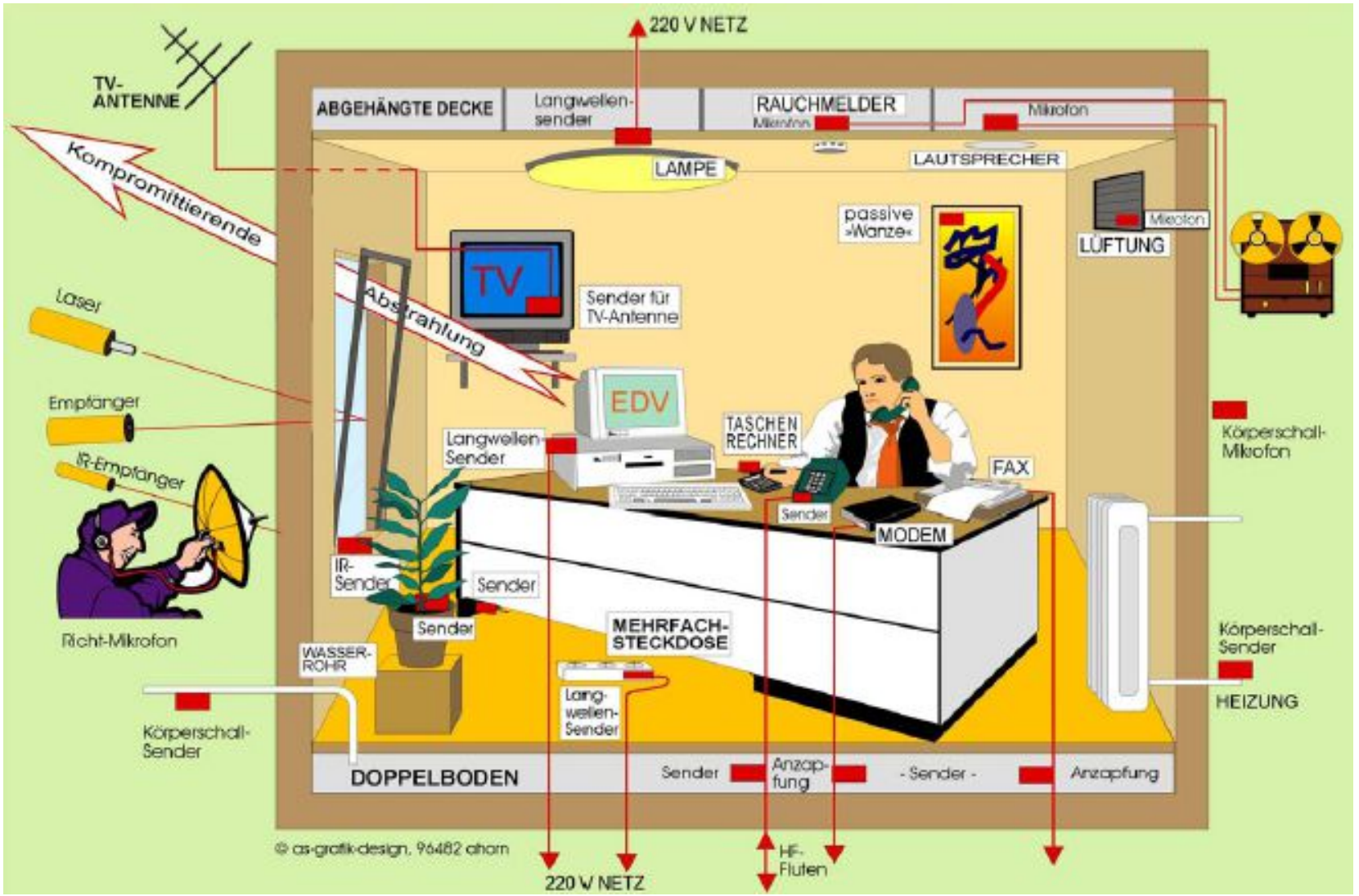
Technik


Letrim
Yakima
Firing Center
Sugar Crove
Menwith Hill
Morwenstow
Misawa
Shoal Bay
Geraldton Station
Waihopai
ECHELON

Technik

- **Kommunikation**
  - **Raumüberwachung**
  - **Einsatz drahtgebundener Mittel**
  - **Abhören mit getarnten Funkwanzen**
  - **Lauschangriffe von Aussen**
  - **Softwareangriffe auf TK-Einrichtungen**

Technik

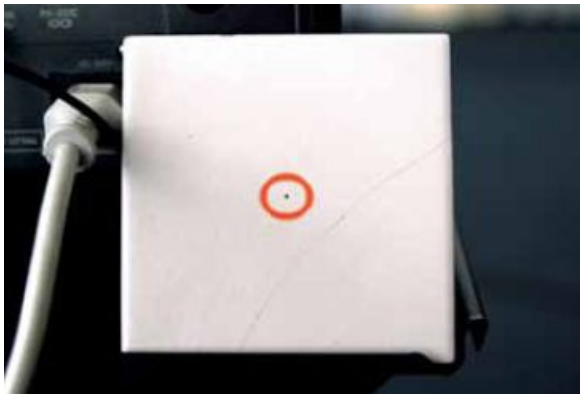

220 V NETZ
TV-ANTENNE
ABGEHÄNGTE DECKE
Langwellen-sender
RAUCHMELDER
Mikrofon
LAMPE
LAUTSPRECHER
Kompromittierende
Abstrahlung
passive »Wanze«
LÜFTUNG
Mikrofon
TV
Sender für TV-Antenne
Laser
Empfänger
IR-Empfänger
EDV
TASCHEN RECHNER
Langwellen Sender
FAX
Körperschall-Mikrofon
Sender
MODEM
IR-Sender
Sender
Sender
MEHRFACH-STECKDOSE
Richt-Mikrofon
WASSER-ROHR
Körperschall-Sender
Lang-wellen-Sender
Körperschall-Sender
HEIZUNG
DOPPELBODEN
Sender
Anzap-fung
- Sender -
Anzapfung
© as-grafik-design, 96482 ahorn
220 V NETZ
HF-Fluten

Technik

Drahtgebunden

Technik

Funk

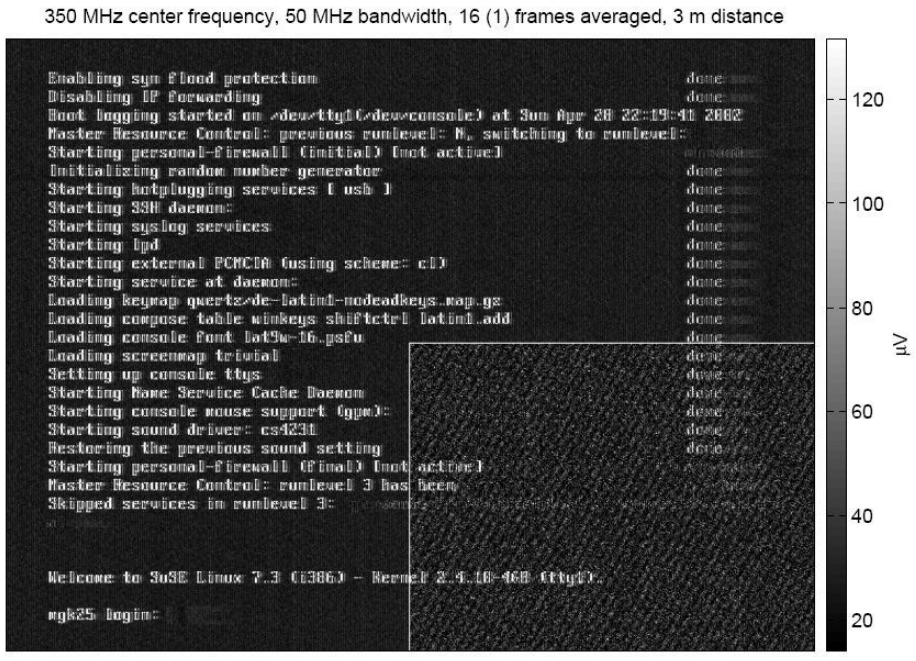


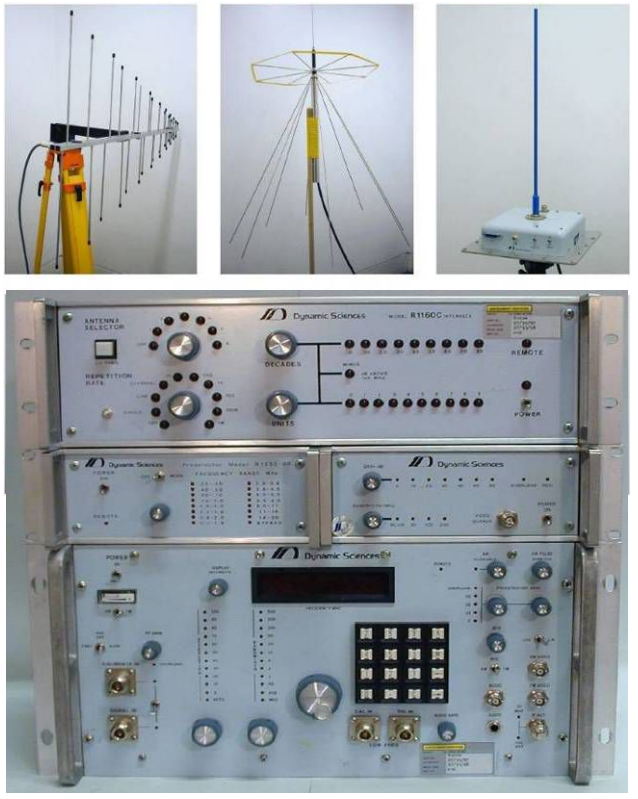
Technik

- **Frequenzen**
  - **VLF 3 kHz – 3 Mhz**
  - **HF 100 kHz – 70 Mhz**
  - **VHF 30 Mhz – 300 Mhz**
  - **UHF 900 Mhz – 3 Ghz**
  - **MWM 3 Ghz – 12.5 Ghz**
  - **MWH 12.5 Ghz – 40 Ghz**
  - **MWmm 40 Ghz – 325 Ghz**
  - **MWmm2 235 Ghz – 1,5 GHz**

Technik

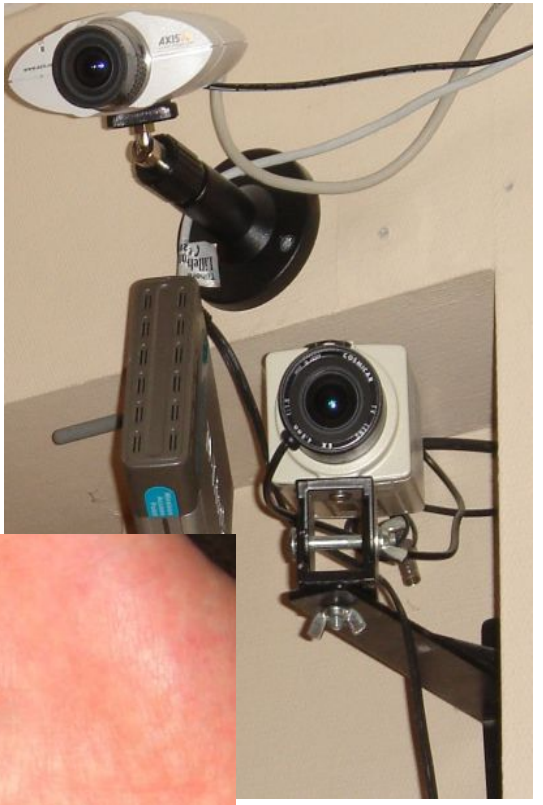
- **TEMPEST**
  - **Temporary Emanation and Spurious Transmission**
  - **Van-Eck-Phreaking (1985)**

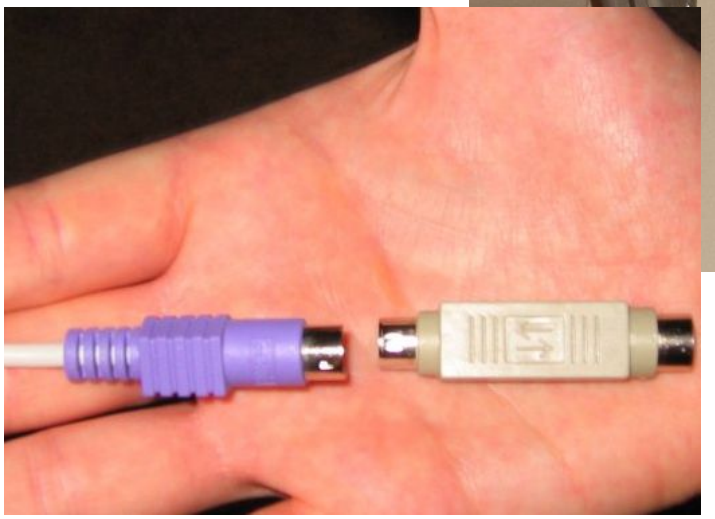




Technik

- **Informatik**
  - **Hardware**
    - **Keylogger**
    - **Kameras, Mikrofone**
  - **Software**
    - **Trojaner, Keylogger**
    - **Covert Channels**
  - **Sniffing**
  - **Hacking**





Alarmsignale 1/3

- Geheimnisse oder Vertrauliches ist bekannt geworden
- Leute scheinen Ihre Aktionen vorauszusehen
- Komische Geräusche/Lautstärkeveränderungen im Telefon
- Telefonhörer (obwohl aufgelegt) macht komische Geräusche
- Telefon läutet, niemand dran (evtl. hoher Ton, Pfiff oder Pieps)
- Ton in Freisprecheinrichtung von Telefon
- AM/FM-Radio oder Fernseher spukt
- Einbruch/Durchsuchung, aber nichts mitgenommen

Alarmsignale 2/3

- **Möbel wurden leicht verrückt**
- **Neues elektronisches Geschenk**
- **Kleine Deformationen Wand, Decke oder Boden**
- **Quasi-reflektierend/gelöchert: Brandmelder, Kamera, Fliese**
- **Gegenstände (Uhr, Sprinkler, EXIT) „plötzlich“ da**
- **Verkleidung von Tisch/Wand oder Decke modifiziert**
- **Telefondienstleister war vor Ort**
- **Servicemitarbeiter (Lüftung, Klima, etc) war vor Ort**

Alarmsignale 3/3

- **Kastenwagen vor Gebäude parkiert**
- **Schlösser sind irgendwie leicht verklemmt**
- **Hinweis/Zugeschickt kriegen von eigenen vertraulichen Daten**
- **Elektrische Schalter/Buchsen sind leicht versetzt**
- **Schatten (münzgross) an Decke oder Wand**
- **Staub oder Verkleidungsstückchen am Boden**

Abwehr Methode

- **Methode**
  - **Kontaktaufnahme (sicher!)**
  - **Kickoff-Meeting (Verdacht, Ziele)**
  - **Vorinspektion**
    - **Baupläne, Inventar, Aussenbegehung**
    - **Verwundbarkeitsanalyse**
    - **Gefahren, Bedrohung, Möglichkeiten, Kommunikationsbeziehungen**

Abwehr Methode

- **Stiller Durchgang**
  - **Passives Detektieren von Wanzen**
- **Aktiver Scan**
  - **Aktives Tracing, Telefonanlage, elektronische Geräte, Wände, Dekor, Kabel**
- **Weitere Schritte**
- **Meldung an Strafverfolgungsbehörden**
- **Report, Präsentation, Pendenzen, Nachbearbeitung**

Abwehr Methode

- Informationstechnologie
  - VoIP, eMail, Covert Channels, Hacking
  - Analyse
    - Resultate, Rückverfolgung
  - Massnahmen
    - Entfernung, Schutz, Verschlüsselung
  - Meldung an Strafverfolgungsbehörden
  - Report, Präsentation, Pendenzen, Nachbearbeitung

Abwehr Massnahmen

- **Organisatorische Massnahmen**
  - **Besucherregelungen**
  - **keine Besucher in Büros!**
  - **Beaufsichtigung von Fremdarbeiten**
  - **Keine Werbe-/Gastgeschenke plazieren**
  - **Verzicht auf vermeidbare Dekorationen**
  - **Zutrittsregelungen für gefährdete Räume**

Abwehr Massnahmen

- **Technische Massnahmen**
  - **Verwendung hochwertiger Aktenvernichter**
  - **Papierabfälle**
  - **Datenträger**
  - **Nutzung hochwertiger Verschlüsselung für alle sensiblen Anwendungen**
  - **Sprache, Fax, Daten, eMail**
  - **Verzicht auf kritische Funkübertragungen**
  - **HF-Schirmung besonders gefährdeter Räume**

Wichtige Fragen

- Wer hätte ein Interesse daran?
  - Feinde, Projekte, Geheimnisse, Motivation
- Welche Informationen sind am interessantesten?
  - Preise, Produkte, Daten
- Wo und wann sind wir am verwundbarsten?
  - Infrastruktur, Kommunikationsverbindungen
- Was haben wir für Verdachtsmomente?
  - Indizes, Unregelmässigkeiten
- Was machen wir, wenn wir etwas finden?
  - Polizei, interne Aktionen

Besten Dank...

… für Ihre Aufmerksamkeit!

Wem darf ich eine Frage beantworten? ;-)

IndianZ
www.indianz.ch