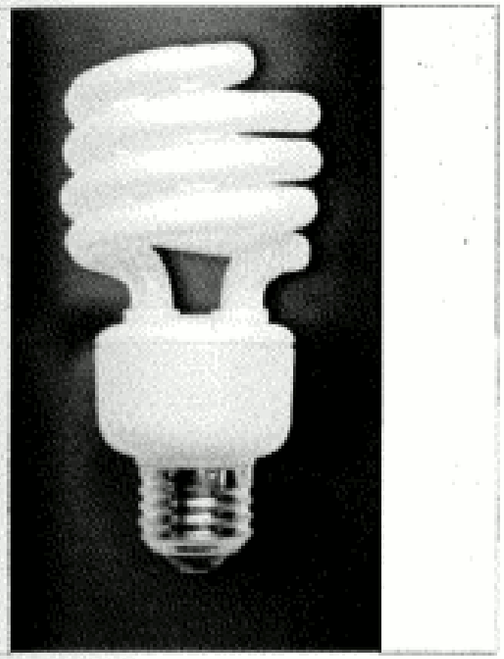
Alles sehen, nix raffen

- Was können die?
- Was können wir dagegen tun?
- Warum haben die uns nicht längst eingedost?
- Was tun?

Spielzeug I



COMPACT AUDIO SURVEILLANCE FLUORESCENT LIGHT SYSTEM

The unit is a unique audio surveillance device capable of operating in hostile environments where the target utilizes TSCM sweep teams to clear the area of "bugs". It utilizes a unique optical communications link capable of stand-off distances of 100m/109yds. Installation merely requires the insertion of the surveillance lamp in the target room. With power applied via the lamp's socket, it collects room audio and transmits it via the optical link to the remote optical receiver. Typical 100m/109yds operating range is limited only by line of sight conditions and environmental ambient lighting such as sun light or bright street lighting next to the target window.

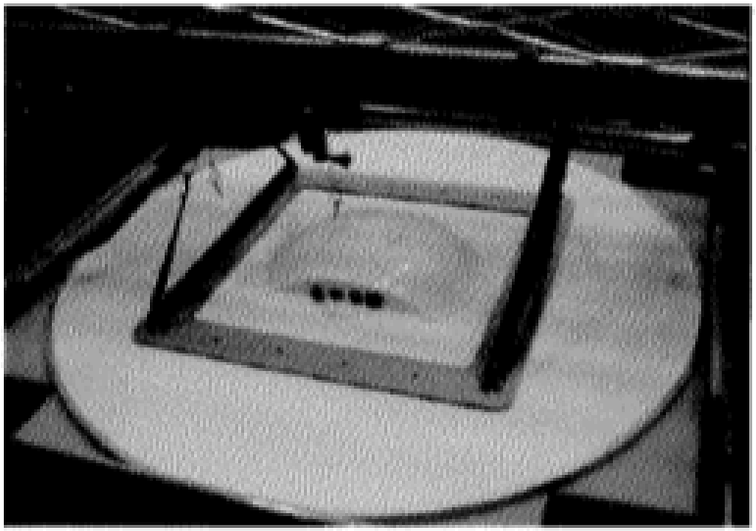
(Aus dem elaman-Katalog)

Spielzeug II

INTUITIVE USER INTERFACE

The system's very intuitive user interface offers fast, accurate operation of the unit. The operator monitors the live on-screen view from the camera, and simply moves the cursor to capture selected audio. The trackball is used to follow moving objects and the jog wheel to go back in time for replay. The system supports multiple output channels and the operator can select up to five listening zones simultaneously – both in real-time and in replay. The operator can also choose to select filters to eliminate undesirable sound and noise.

Mobile System installed in a car tire

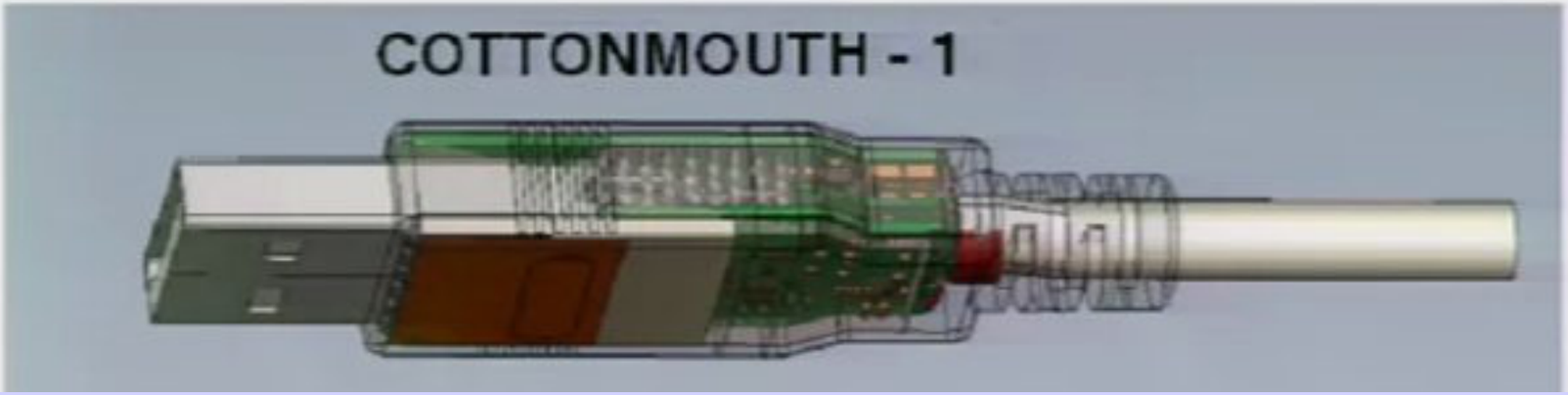


Fixed System installed in a room ceiling

(Aus dem elaman-Katalog)

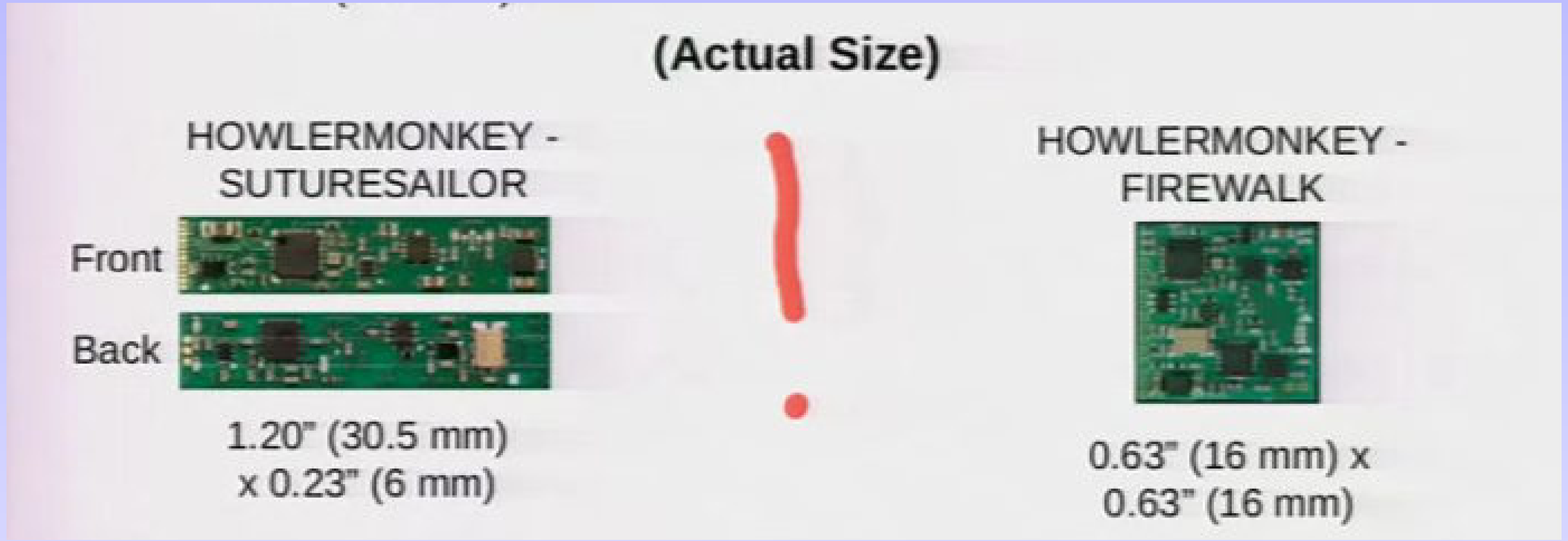
Spielzeug III

(TS//SI//REL) COTTONMOUTH-I (CM-I) is a Universal Serial Bus (USB) hardware implant which will provide a wireless bridge into a target network as well as the ability to load exploit software onto target PCs.



(Aus den Snowden-Leaks)

Spielzeug IV



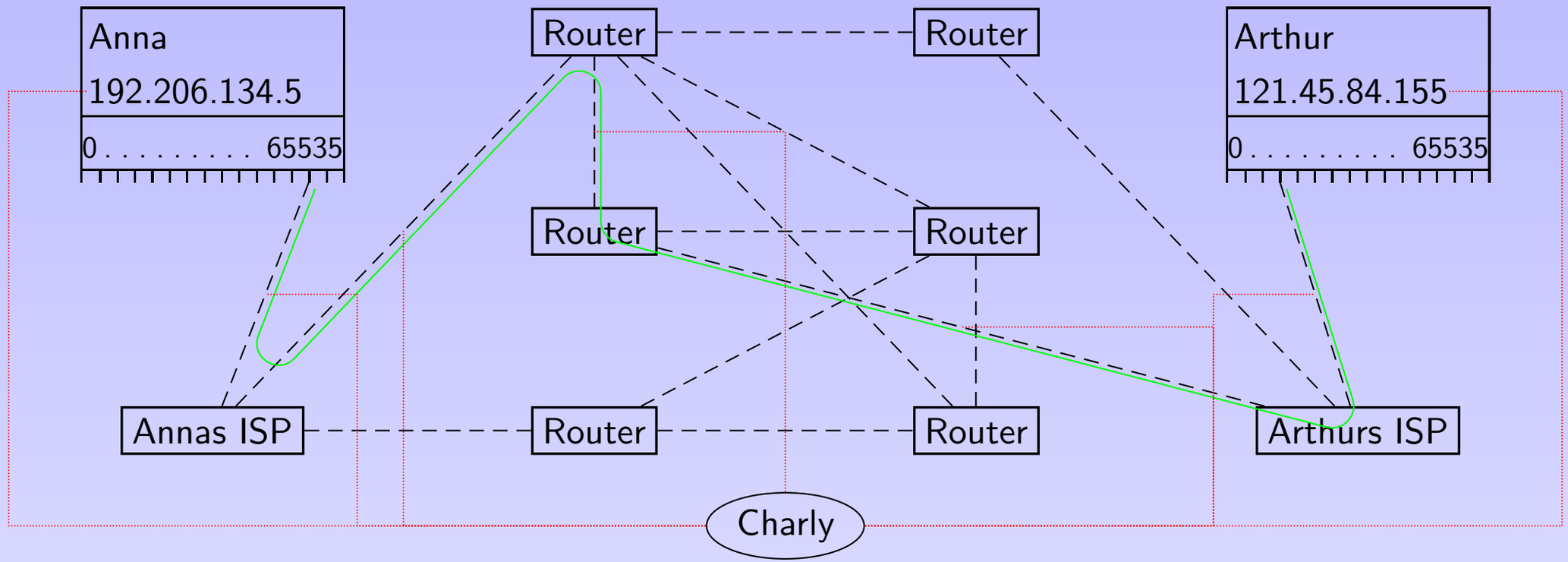
(aus den Snowden-Leaks)

Spielzeug V

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

(aus den Snowden-Leaks)

Breit/flach vs. eng/tief



Die roten Linien zeigen, wo Charly überall abhören kann:

- Direkt in den Rechnern von Anna oder Arthur
- An den Leitungen von den Leuten zu ihren ISPs
- An den Übergabepunkten der ISPs ins Internet
- An den Backbones

Was können wir tun?

Im Jargon: „Operational Security“ (OpSec) und „Tactical Surveillance Counter Measures“ (TSCM)

Gegen einen gezielten Angriff *würde* helfen:

- Alle Kommunikation stark verschlüsseln mit sorgfältigem Schlüsselmanagement
- Alles Ausführbare nur von vertrauenswürdigen Quellen mit ordentlicher Krypto beziehen
- Physischen Zugriff durch Behörden auf alle Hardware verhindern, spätestens ab Kauf
- Alles Vertrauliche in stromlosen, schallgeschützten Räumen ausmachen

Aufgeben?

Wenn die alles können, warum kriegen sie dann nichts auf Reihe?

- Abwegiger Mist in VS-Berichten
- Erfolgreiche Aktionen gegen z.B. Bundeswehrkram, die allenfalls durch Zufall aufgeklärt werden
- Zehn Jahre Suche nach Bin Laden, weitgehend unbehinderte Operationen von Taliban und Freunden, hilfloses Drohnen-Rumgeballere
- Nicht mal Vollamateure wie die Marathon-Bomber werden erwischt.
- V-Mann ist bei Nazi-Mord dabei

Malfunction

Mögliche Gründe für Dienste-Murks:

- Wettbewerb in den Behörden und zwischen den Behörden
- Politische gewollte aber abwegige Theorien (z.B. „Extremismus“)
- Quasireligöse Verblendung wichtiger Mitarbeiter („Antikommunismus“), innere Emigration
- Unfähigkeit im Umgang mit Technik
- Ökonomie des sicherheits-industriellen Komplexes
- (In der BRD:) Eher überschaubare Ressourcen

Geheimdienst spielen?

Die Dienste machen nicht viele all-out *Einzelangriffe* (brauchen trotz Computern ≥ 1 Dienstler pro Opfer).

Aber: Abwehr von *Massenüberwachung* ist realistisch und notwendig:

- Telefon so oft wie möglich funklos machen
- So viel wie möglich verschlüsseln (PGP, SSL wenn möglich mit Certificate Patrol)
- So wenig App- und Download-Mist wie halt möglich
- Verstand verwenden

Bringts was?

Die Dienste können die Krypto unter richtig verwendetem PGP und SSL *nicht* brechen.

Wenn überhaupt, können sie die Schlüsselverwaltung angreifen („MITM“). Bei PGP ist das eher schwierig, bei SSL eher leicht.

Die Dienste greifen *sicher* routinemäßig auf Telekom-Metadaten zu. Lange vor einem gezielten Angriff werden sie die nutzen. Oh: Für Raumüberwachung durchs Telefon gibts in der BRD immer noch keinen Beleg.

Aber

Die Dienste funktionieren, obwohl sie murksen:

Fear, Uncertainty, Doubt

- Angst: Wenn ich mein Maul aufmache, fliege ich dann?
- Unsicherheit: Können die mich hier hören?
- Zweifel: Ist Arthur vielleicht ein Spitzel?

Die Angst vor dem Handeln der Geheimdienste ist weit schlimmer als das, was sie wirklich tun.

Das panoptische Prinzip

Die historische Gelegenheit

Die Abschaffung oder Einschränkung der Geheimdienste ist entscheidend für unsere Handlungsfähigkeit.

Die Dienste sind aber nach NSU und Co schon angeschlagen. Auch der Obrigkeit ist aufgefallen, dass sie nicht so funktionieren, wie sie behaupten.

Die Macht der Dienste über die Obrigkeit ist aber auch nicht zu unterschätzen.

Es liegt an uns, Druck zu machen, den Skandal Geheimdienste immer weiter zu thematisieren, mit allem, was wir so an Aktionsformen haben.