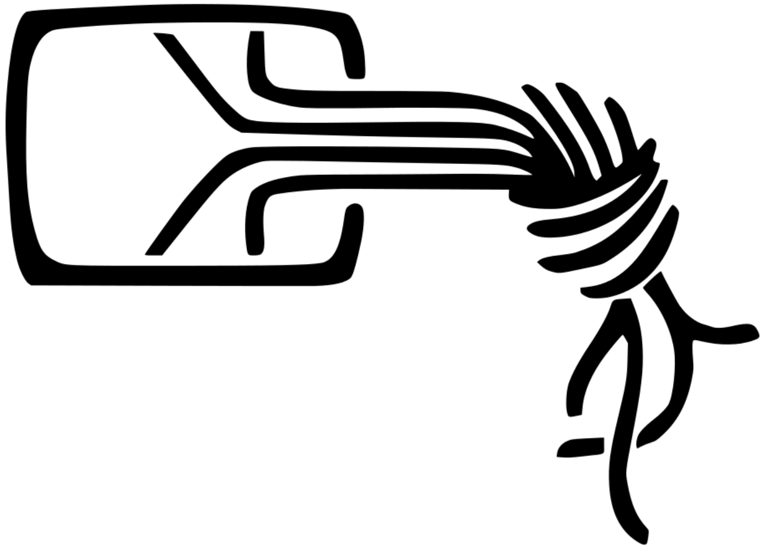
Thématiques récentes du Chaos Computer Club/Congress

partie 2



2012

29C3 - Not my department

2013

30C3

NICELAB_

Nicelab, Laboratoire Ouvert de Nice, Hackerspace, depuis 2011

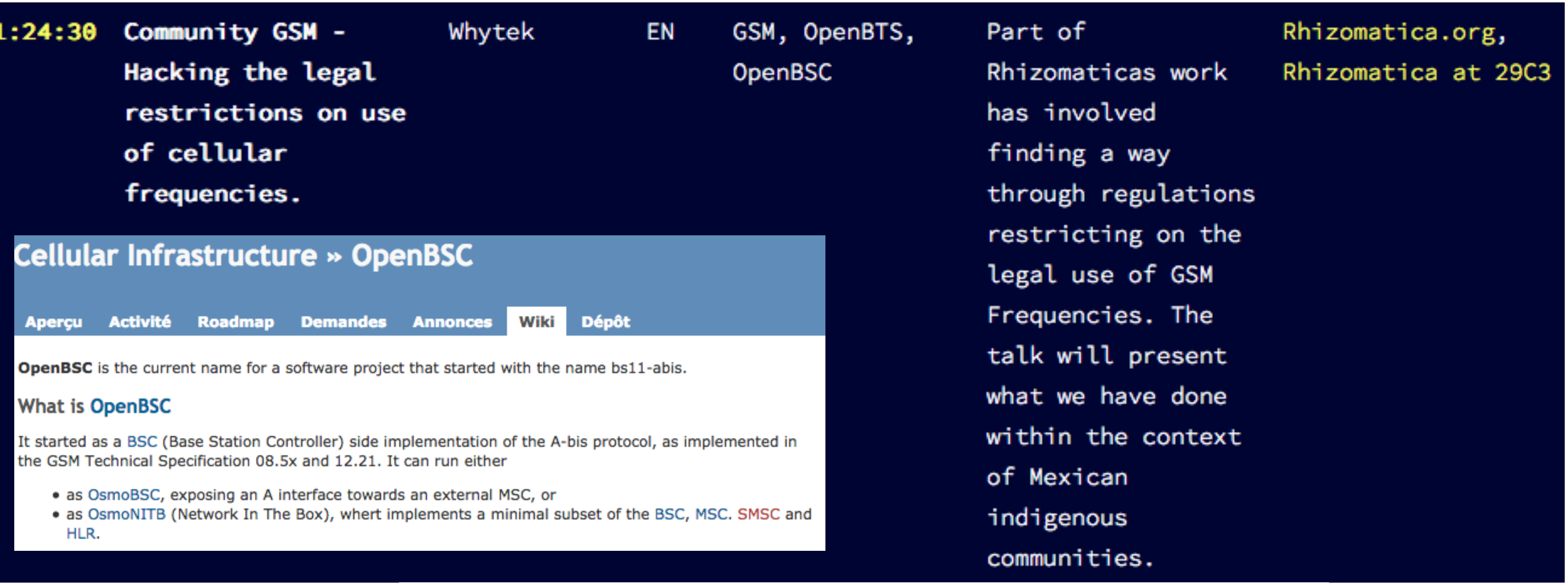
Once-the.rockets/are-up..who/
cares-where.they/
come.down.That's

N.O-T/MY-D/E.PA/R.T-ME-N/T.

2.9-C/3

2012- 29C3 - Not my department

rhizomatica.org



1:24:30	Community GSM - Hacking the legal restrictions on use of cellular frequencies.	Whytek	EN	GSM, OpenBTS, OpenBSC	Part of Rhizomaticas work has involved finding a way through regulations restricting on the legal use of GSM Frequencies. The talk will present what we have done within the context of Mexican indigenous communities.	Rhizomatica.org, Rhizomatica at 29C3

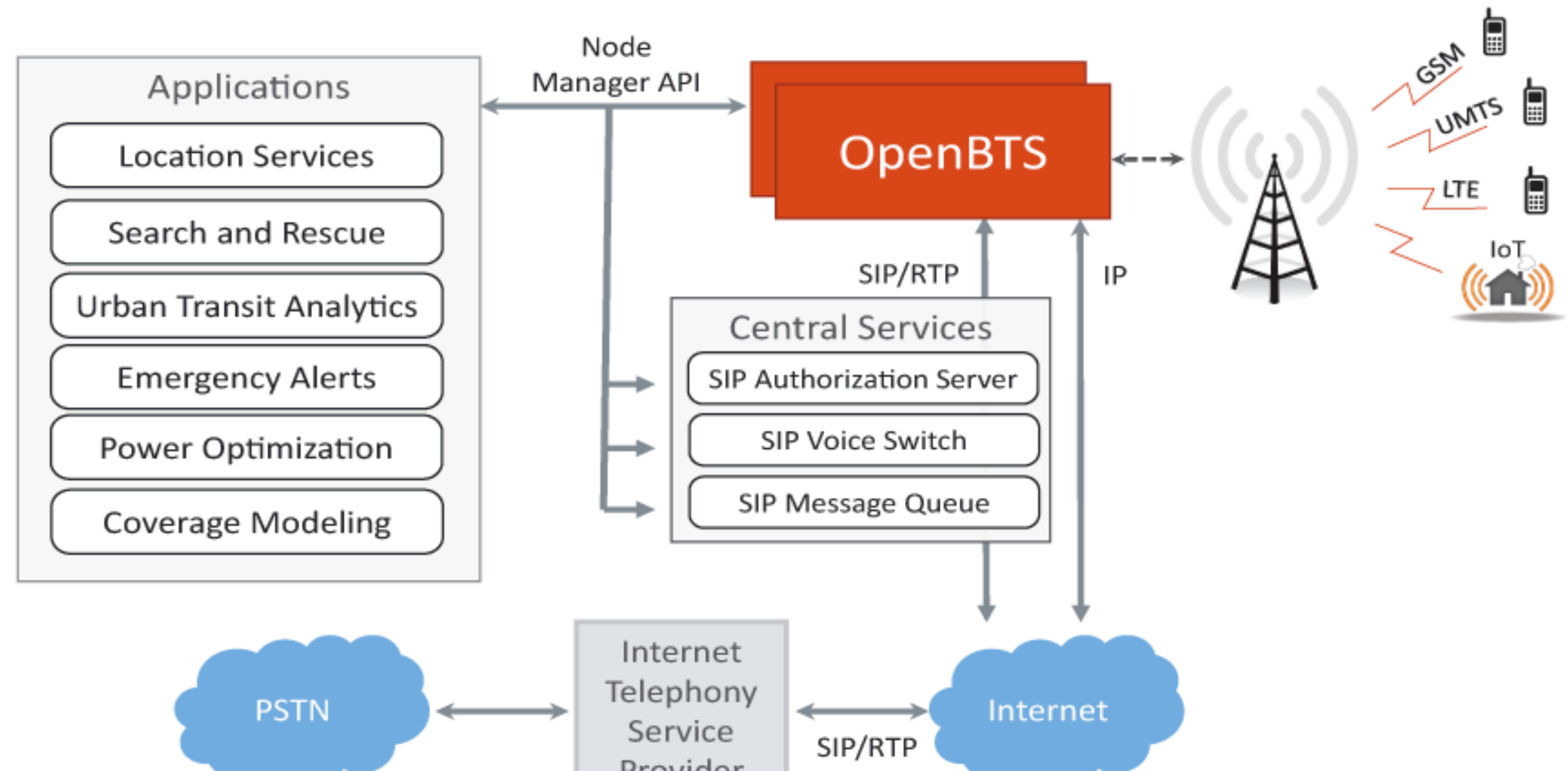
Cellular Infrastructure » OpenBSC

OpenBSC is the current name for a software project that started with the name bs11-abis.

What is OpenBSC

It started as a BSC (Base Station Controller) side implementation of the A-bis protocol, as implemented in the GSM Technical Specification 08.5x and 12.21. It can run either

- as OsmoBSC, exposing an A interface towards an external MSC, or
- as OsmoNITB (Network In The Box), whert implements a minimal subset of the BSC, MSC. SMSC and HLR.



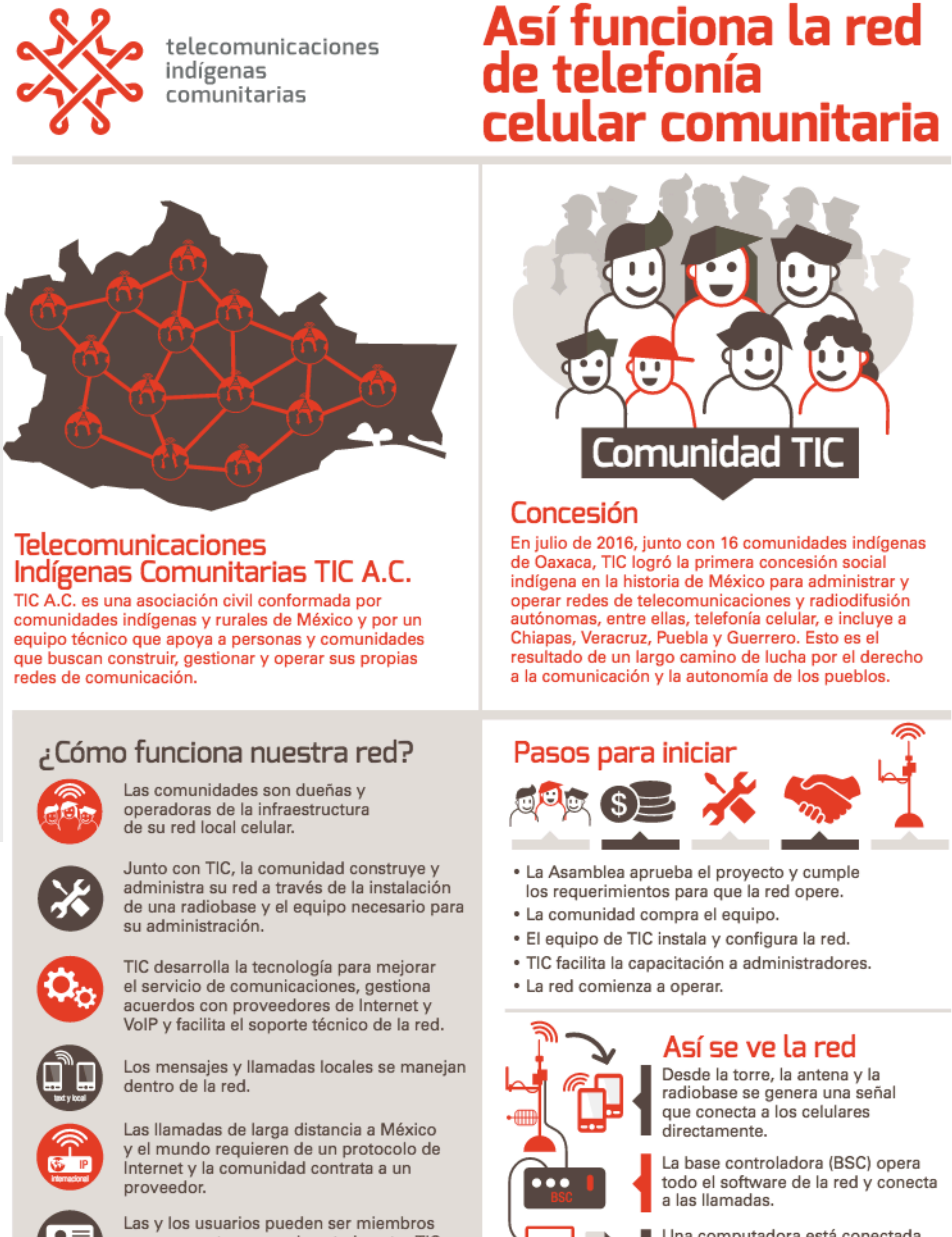
2012- 29C3 - Not my department

Telecomunicaciones Indígenas Comunitarias

Oaxaca

Projet de Réseau GSM associatif autogéré

that an indigenous community in the middle of the mountains


Comunidad TIC
text y local
IP
Internacional
BSC

telecomunicaciones indígenas comunitarias

Así funciona la red de telefonía celular comunitaria

Telecomunicaciones Indígenas Comunitarias TIC A.C.

TIC A.C. es una asociación civil conformada por comunidades indígenas y rurales de México y por un equipo técnico que apoya a personas y comunidades que buscan construir, gestionar y operar sus propias redes de comunicación.

Concesión

En julio de 2016, junto con 16 comunidades indígenas de Oaxaca, TIC logró la primera concesión social indígena en la historia de México para administrar y operar redes de telecomunicaciones y radiodifusión autónomas, entre ellas, telefonía celular, e incluye a Chiapas, Veracruz, Puebla y Guerrero. Esto es el resultado de un largo camino de lucha por el derecho a la comunicación y la autonomía de los pueblos.

¿Cómo funciona nuestra red?

Las comunidades son dueñas y operadoras de la infraestructura de su red local celular.

Junto con TIC, la comunidad construye y administra su red a través de la instalación de una radiobase y el equipo necesario para su administración.

TIC desarrolla la tecnología para mejorar el servicio de comunicaciones, gestiona acuerdos con proveedores de Internet y VoIP y facilita el soporte técnico de la red.

Los mensajes y llamadas locales se manejan dentro de la red.

Las llamadas de larga distancia a México y el mundo requieren de un protocolo de Internet y la comunidad contrata a un proveedor.

Las y los usuarios pueden ser miembros

Pasos para iniciar

- La Asamblea aprueba el proyecto y cumple los requerimientos para que la red opere.
- La comunidad compra el equipo.
- El equipo de TIC instala y configura la red.
- TIC facilita la capacitación a administradores.
- La red comienza a operar.

Así se ve la red

Desde la torre, la antena y la radiobase se genera una señal que conecta a los celulares directamente.

La base controladora (BSC) opera todo el software de la red y conecta a las llamadas.

Una computadora está conectada

2012- 29C3 - Not my department

rhizomatica.org

The Serval Project is a small team of academics, contracted engineers and students in the Resilient Networks Lab of Flinders University in South Australia, developing revolutionary, free, open-source software for mobile telephones.

- Wiki editing policy – how to contribute to this wiki

Serval Mesh

Serval Mesh is an Android app that provides highly secure mesh networking, voice calls, text messaging and file sharing between m
any other infrastructure like mobile cell towers, Wi-Fi hotspots or Internet access.

- Serval Mesh general information – download, install, documentation, release
- Serval Mesh development – copyright, source code, technical documentatio
- Supported Devices – supported Android phones and devices
- Serval DNA (core component) – general information
- Serval DNA development – copyright, source code and branching, technical

Serval Chat

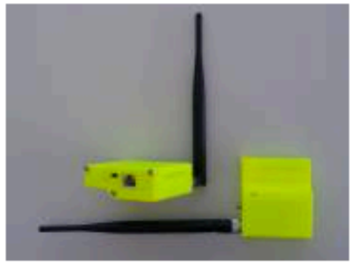
Serval Chat is an iOS app that provides highly secure text messaging between Apple iPhone ar

- for the time being, Serval Chat does not communicate with the Serval Mesh app for Android

Serval Maps

Serval Maps is an Android app that uses Serval Mesh to provide collaborative, infrastructure-in

Serval Mesh Extender (Formerly Mesh Helper)



The **Serval Mesh Extender** is a hardware device that helps other

Second-Generation Mesh Extenders:

- powered by external USB, 12v/24v automotive and/or solar (with
- Integrated LiFEPO4/Lilon/Sealed-Lead-Acid battery charger
- Custom-designed injection-moulded housing
- Designed to meet IP66 environmental resistance
- Integrated “Mesh of Things”/“Internet of Things” I/O port

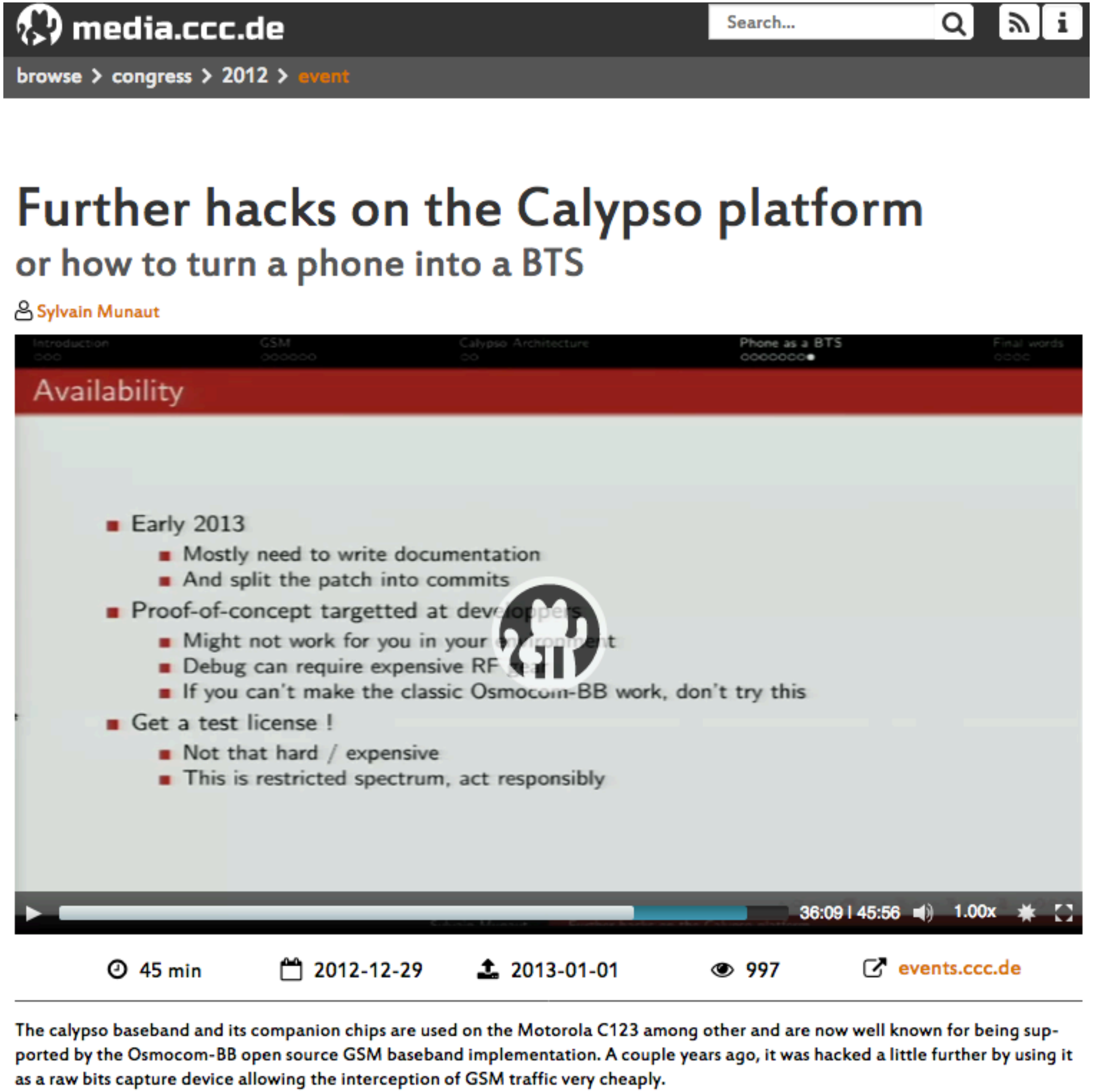
The main focus to date has been on developing the free **Serval Mesh (app for Android)** to provide voice calls, text messaging and file sharing directly over Wi-Fi links between phones. The app communicates with distant phones via intermediate phones using mesh routing, and uses strong elliptic curve encryption to guarantee privacy and identity even though some phones in the mesh network may not be trusted.

The Serval Project is developing the **Serval Mesh Extender** device to overcome the range limitations of Wi-Fi on smart-phones and to extend Serval Mesh services to handsets other than just Android devices. This will allow more kinds of smart-phones to participate in the Serval Mesh.

The Serval Project also develops the free **Serval Maps (app for Android)** which uses Serval Mesh file sharing to provide decentralised mapping. This is a useful situational awareness tool for emergency response teams.

Serval Project au Vanuatu

2012- 29C3 - Not my department



Further hacks on the Calypso platform

or how to turn a phone into a BTS

Sylvain Munaut

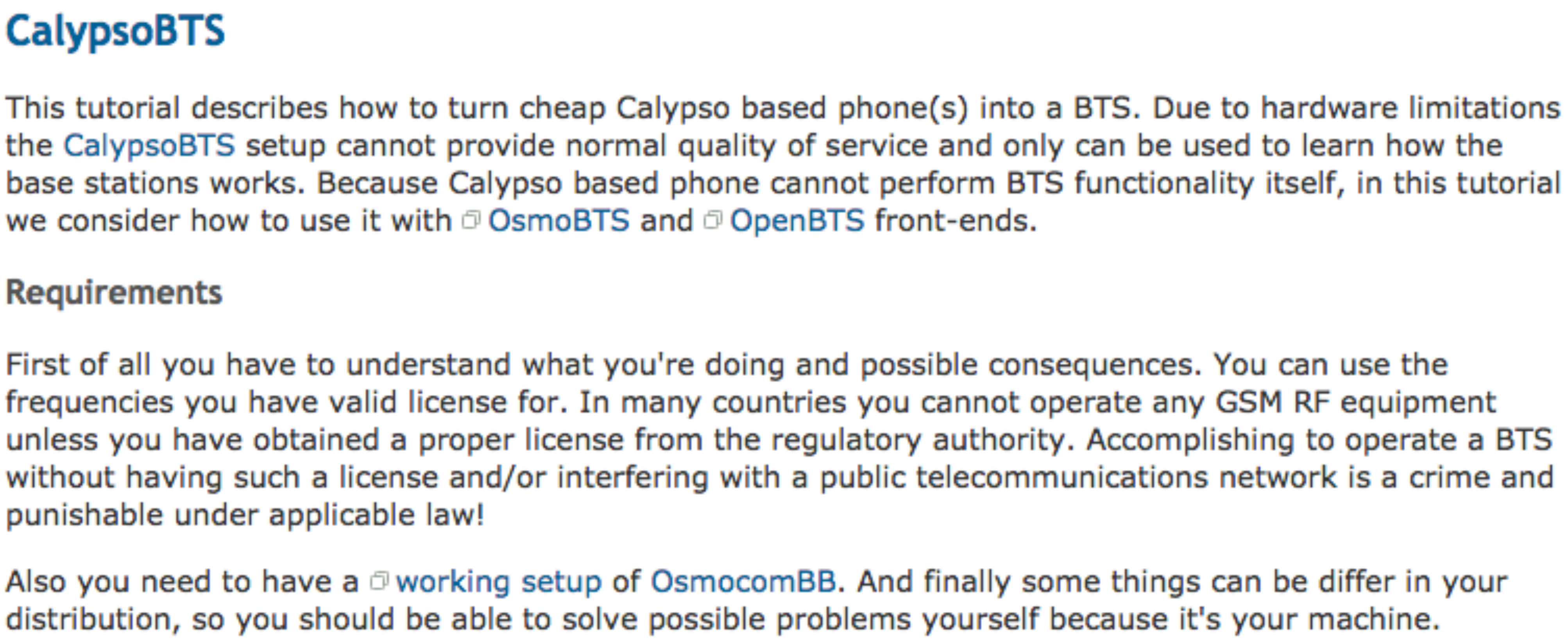
Availability

- Early 2013
  - Mostly need to write documentation
  - And split the patch into commits
- Proof-of-concept targetted at developers
  - Might not work for you in your environment
  - Debug can require expensive RF gear
  - If you can't make the classic Osmocom-BB work, don't try this
- Get a test license !
  - Not that hard / expensive
  - This is restricted spectrum, act responsibly

45 min | 2012-12-29 | 2013-01-01 | 997 | events.ccc.de

The calypso baseband and its companion chips are used on the Motorola C123 among other and are now well known for being supported by the Osmocom-BB open source GSM baseband implementation. A couple years ago, it was hacked a little further by using it as a raw bits capture device allowing the interception of GSM traffic very cheaply.

2012- 29C3 - Not my department



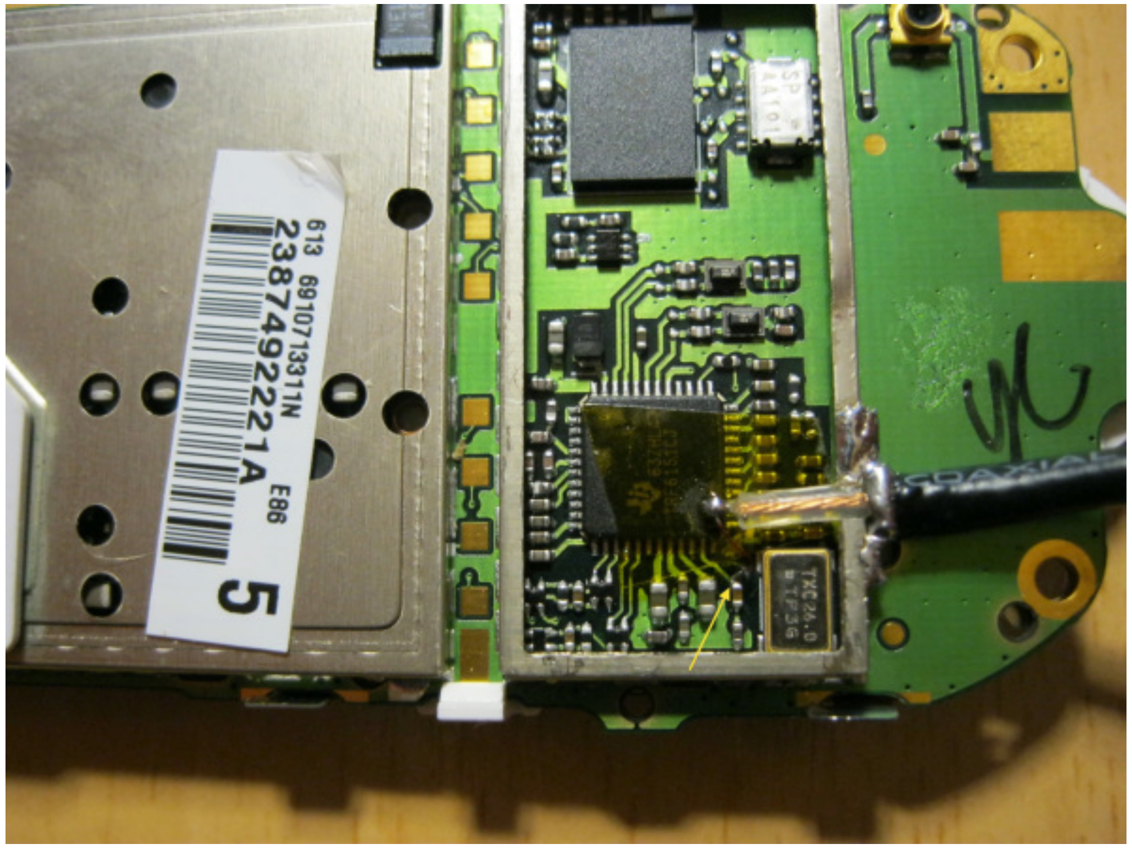
CalypsoBTS

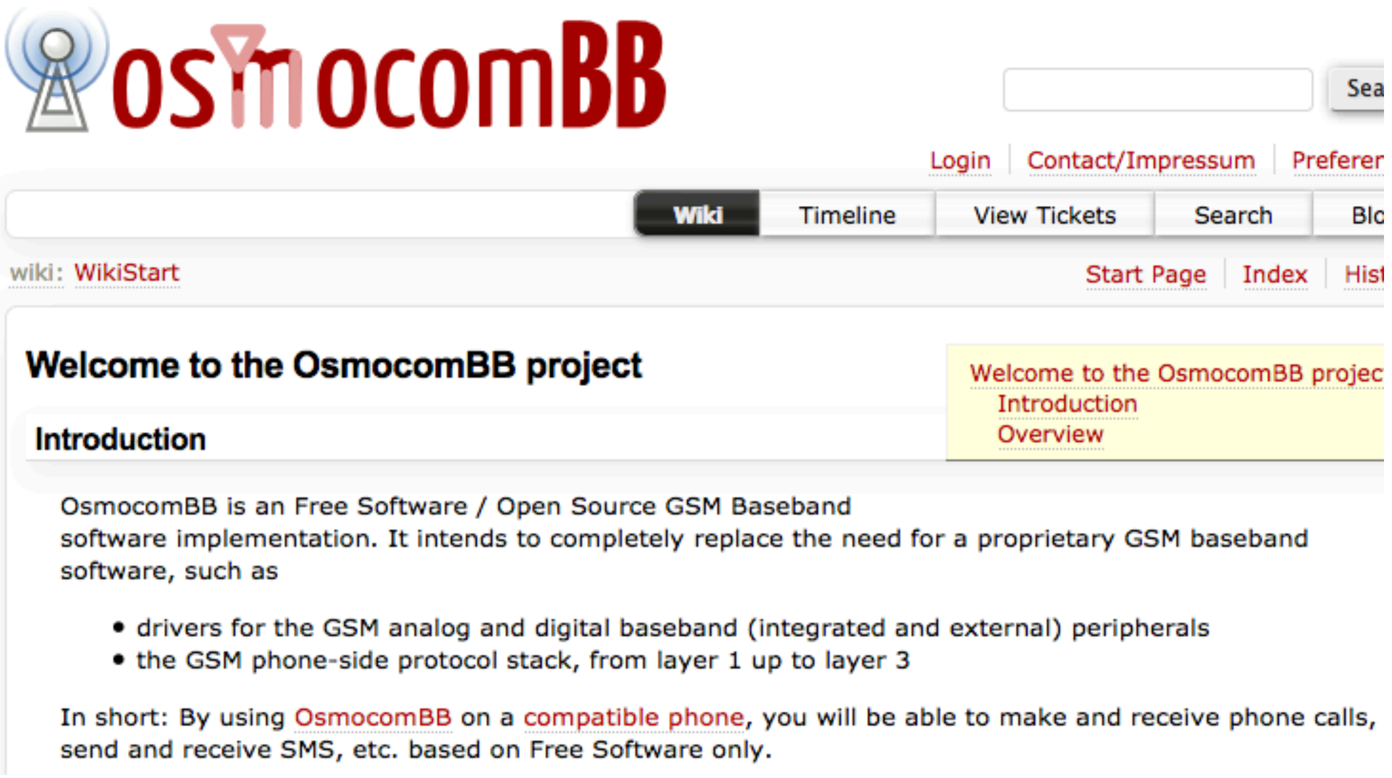
This tutorial describes how to turn cheap Calypso based phone(s) into a BTS. Due to hardware limitations the CalypsoBTS setup cannot provide normal quality of service and only can be used to learn how the base stations works. Because Calypso based phone cannot perform BTS functionality itself, in this tutorial we consider how to use it with OsmoBTS and OpenBTS front-ends.

Requirements

First of all you have to understand what you're doing and possible consequences. You can use the frequencies you have valid license for. In many countries you cannot operate any GSM RF equipment unless you have obtained a proper license from the regulatory authority. Accomplishing to operate a BTS without having such a license and/or interfering with a public telecommunications network is a crime and punishable under applicable law!

Also you need to have a working setup of OsmocomBB. And finally some things can be differ in your distribution, so you should be able to solve possible problems yourself because it's your machine.





Welcome to the OsmocomBB project

Introduction

OsmocomBB is an Free Software / Open Source GSM Baseband software implementation. It intends to completely replace the need for a proprietary GSM baseband software, such as

- drivers for the GSM analog and digital baseband (integrated and external) peripherals
- the GSM phone-side protocol stack, from layer 1 up to layer 3

In short: By using OsmocomBB on a compatible phone, you will be able to make and receive phone calls, send and receive SMS, etc. based on Free Software only.

2012- 29C3 - Not my department

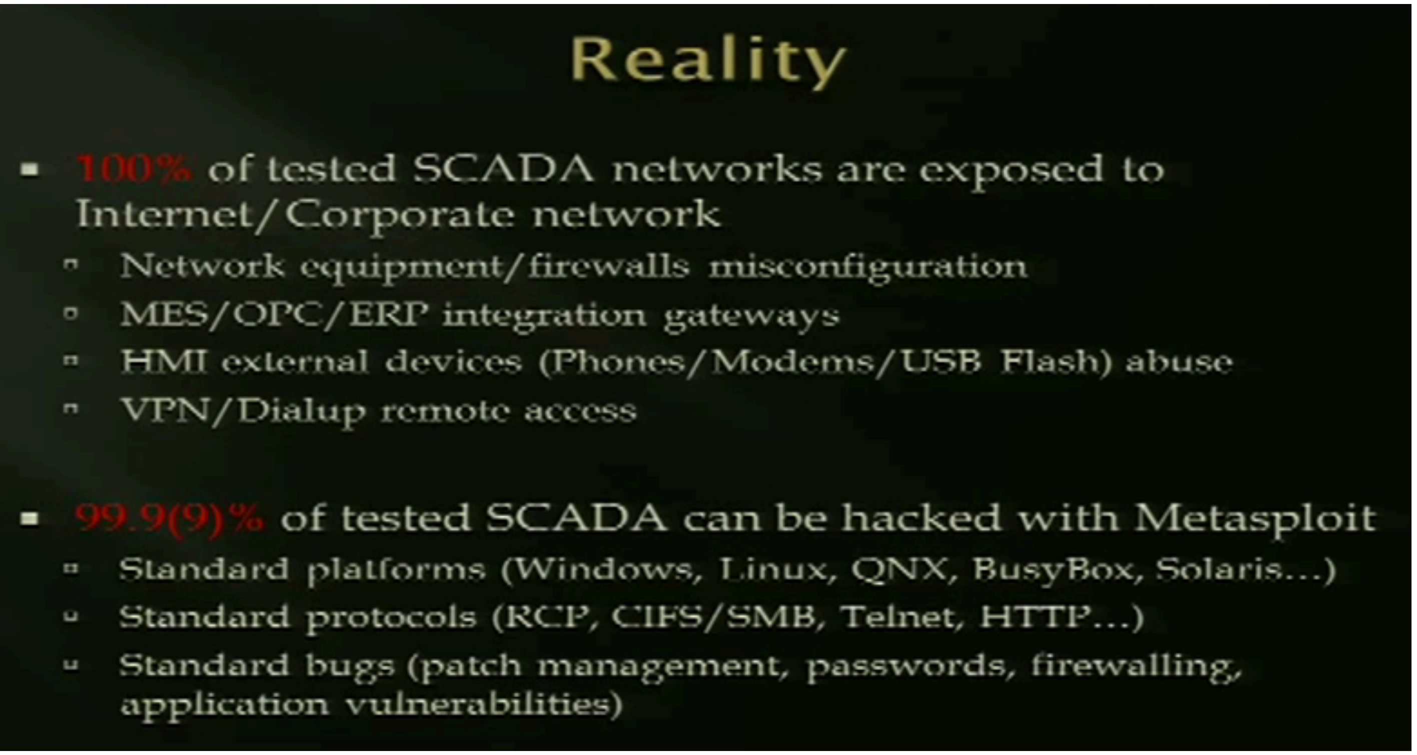
(supervisory control and data acquisition)

SCADA Strangelove

or: How I Learned to Start Worrying and Love Nuclear Plants

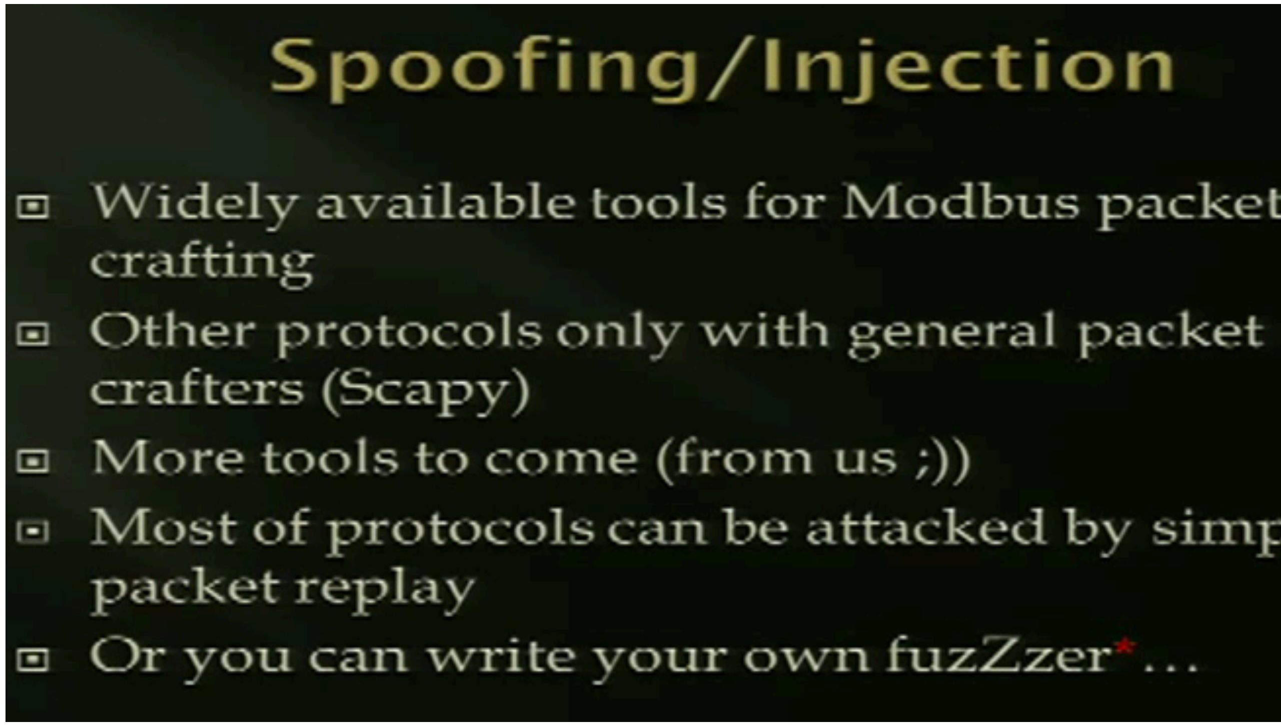
Denis Baranov, Gleb Gritsai and Sergey Gordeychik

Modern civilization unconditionally depends on information systems. It is paradoxical but true that ICS/SCADA systems are the most insecure systems in the world. From network to application, SCADA is full of configuration issues and vulnerabilities.



Reality

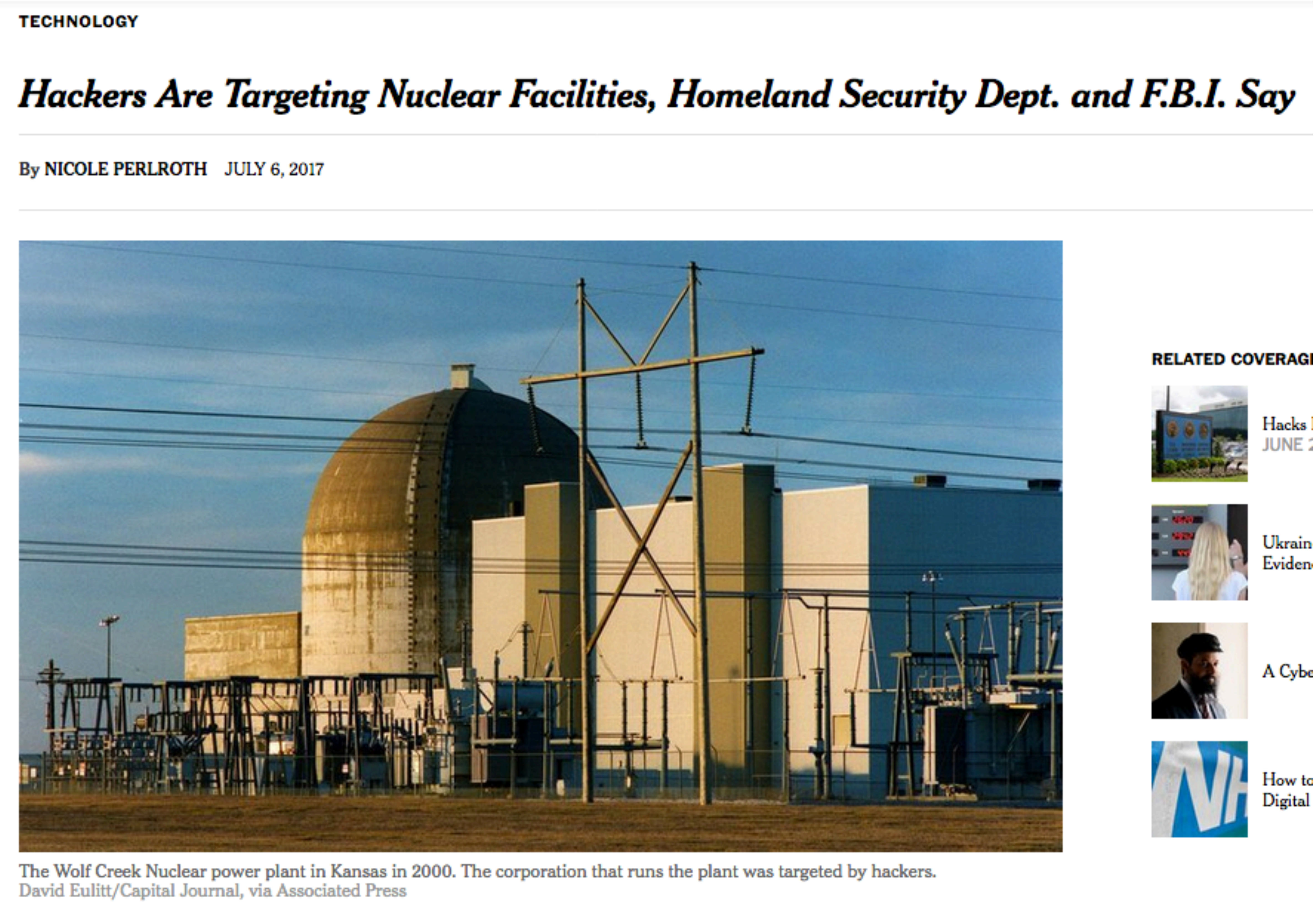
- 100% of tested SCADA networks are exposed to Internet/Corporate network
  - Network equipment/firewalls misconfiguration
  - MES/OPC/ERP integration gateways
  - HMI external devices (Phones/Modems/USB Flash) abuse
  - VPN/Dialup remote access
- 99.9(9)% of tested SCADA can be hacked with Metasploit
  - Standard platforms (Windows, Linux, QNX, BusyBox, Solaris...)
  - Standard protocols (RCP, CIFS/SMB, Telnet, HTTP...)
  - Standard bugs (patch management, passwords, firewalling, application vulnerabilities)



Spoofing/Injection

- ▣ Widely available tools for Modbus packet crafting
- ▣ Other protocols only with general packet crafters (Scapy)
- ▣ More tools to come (from us ;))
- ▣ Most of protocols can be attacked by simp packet replay
- ▣ Or you can write your own fuzZzer*...

2012- 29C3 - Not my department



TECHNOLOGY

Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say

By NICOLE PERLROTH JULY 6, 2017

The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers.
David Eulitt/Capital Journal, via Associated Press

RELATED COVERAGI

Hacks I
JUNE 2

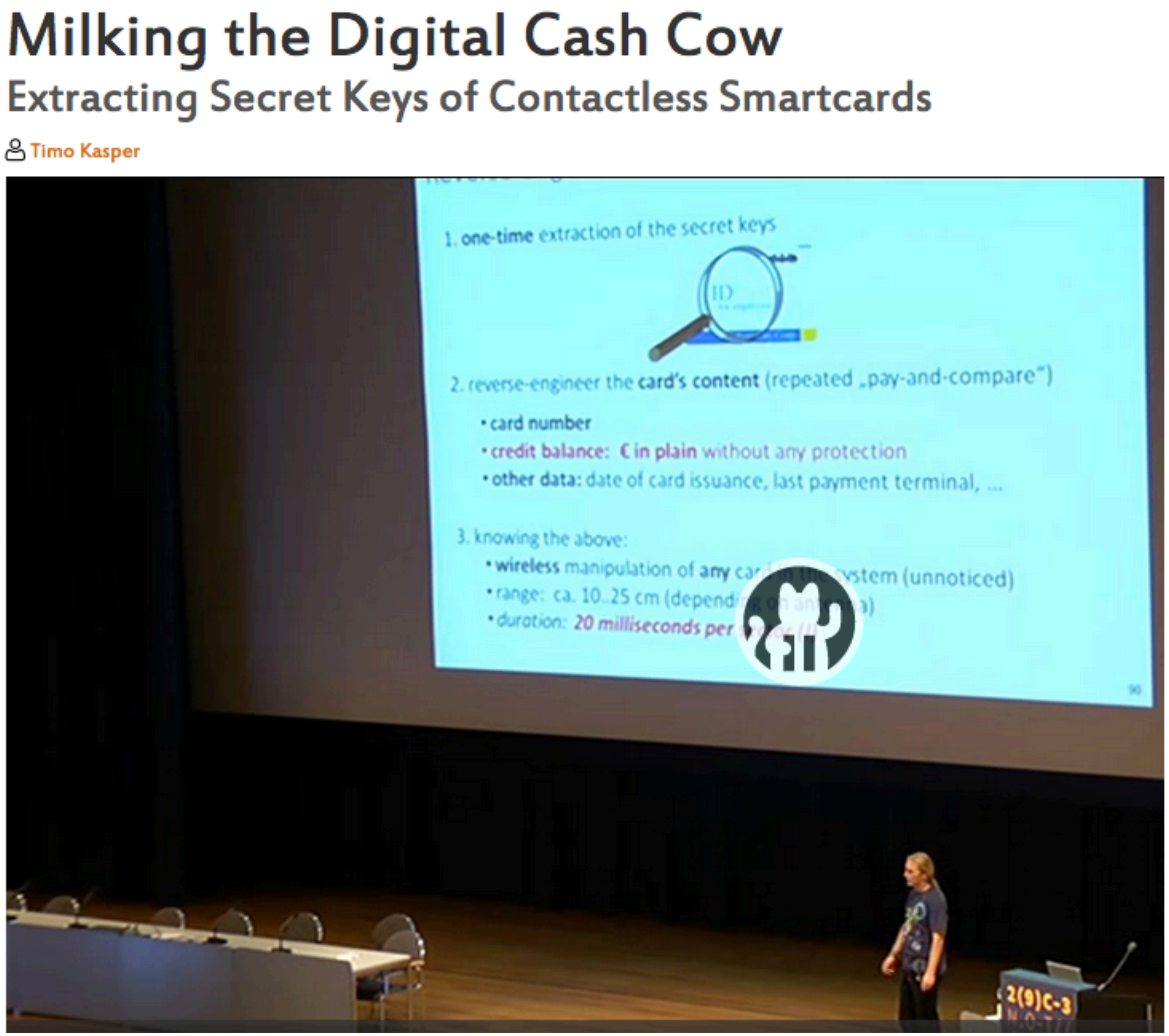
Ukrain
Eviden

A Cybe

How to
Digital

But like any software, Scada systems are susceptible to hacking and computer viruses. And for years, security specialists have warned that hackers could use remote access to these systems to cause physical destruction.

2012- 29C3 - Not my department



Milking the Digital Cash Cow

Extracting Secret Keys of Contactless Smartcards

Timo Kasper

1. **one-time** extraction of the secret keys
2. reverse-engineer the **card's content** (repeated „pay-and-compare")
   - **card number**
   - **credit balance: € in plain** without any protection
   - **other data:** date of card issuance, last payment terminal, ...
3. knowing the above:
   - **wireless** manipulation of **any** card in the system (unnoticed)
   - range: ca. 10..25 cm (depending on antenna)
   - duration: *20 milliseconds per sector (!)*

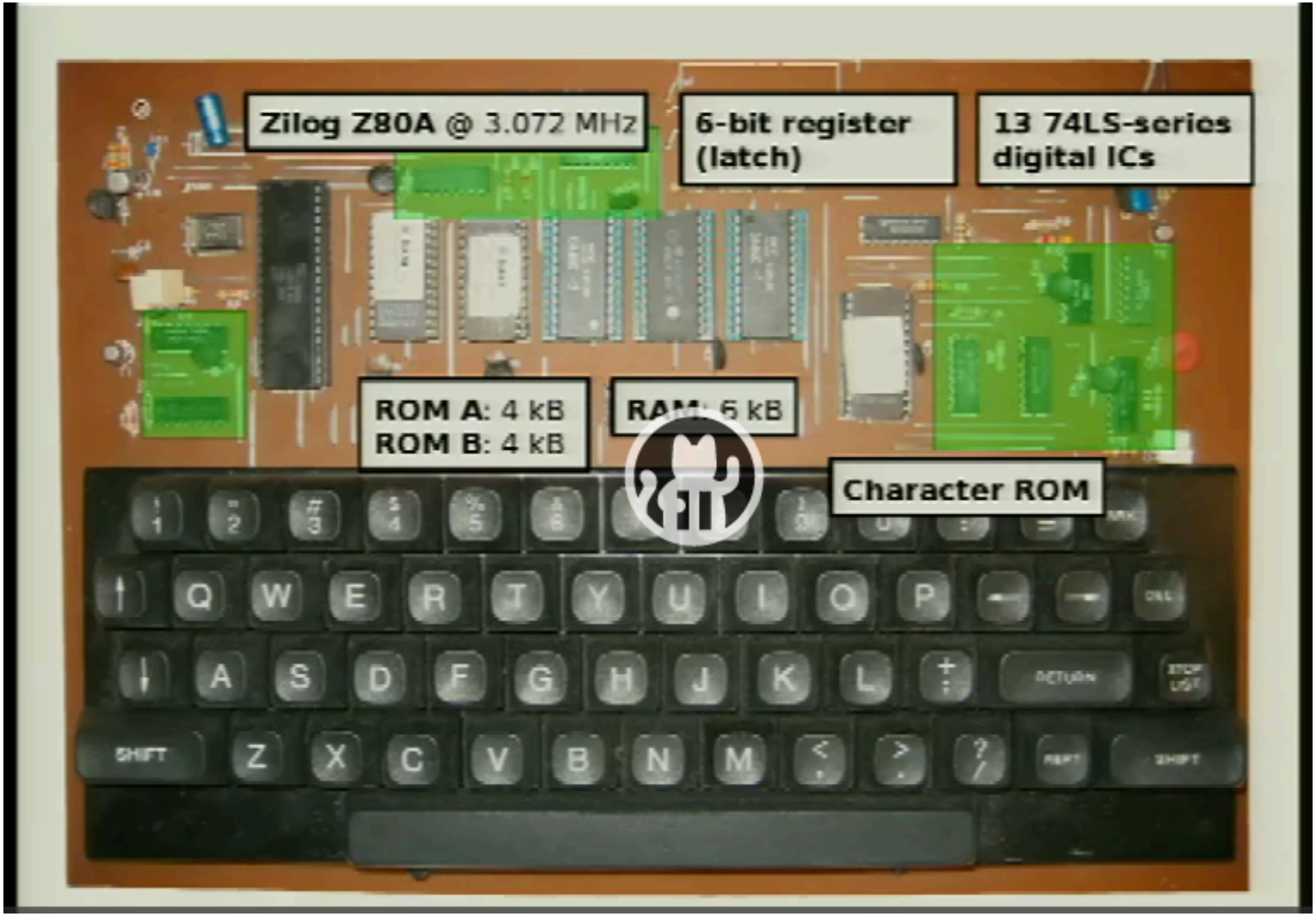
Contactless smartcards have become widespread for applications such as ticketing, access control, identification and payments. Side-channel analysis (SCA) is a powerful type of passive implementation attack that enables to extract the secret keys of cryptographic devices. At the example of NXP's Mifare DESfire MF3ICD40 smartcards we demonstrate that SCA attacks can be applied to cryptographic RFID devices: By exploiting the electro-magnetic information leakage of the cards, its cryptographic keys are revealed.

We introduce our open-source tools for analyzing contactless smartcards, i.e., an ISO 14443 RFID reader (http://sourceforge.net/projects/reader14443) and the card emulator Chameleon (http://sourceforge.net/projects/chameleon14443). We then present the probably worst realization of a commercial contactless payment system ever and detail on various real-world attacks on this widespread (in Germany) system, e.g., how to 'milk the digital cash cow' by modifying the credit balance and convert zeros and ones into real money.

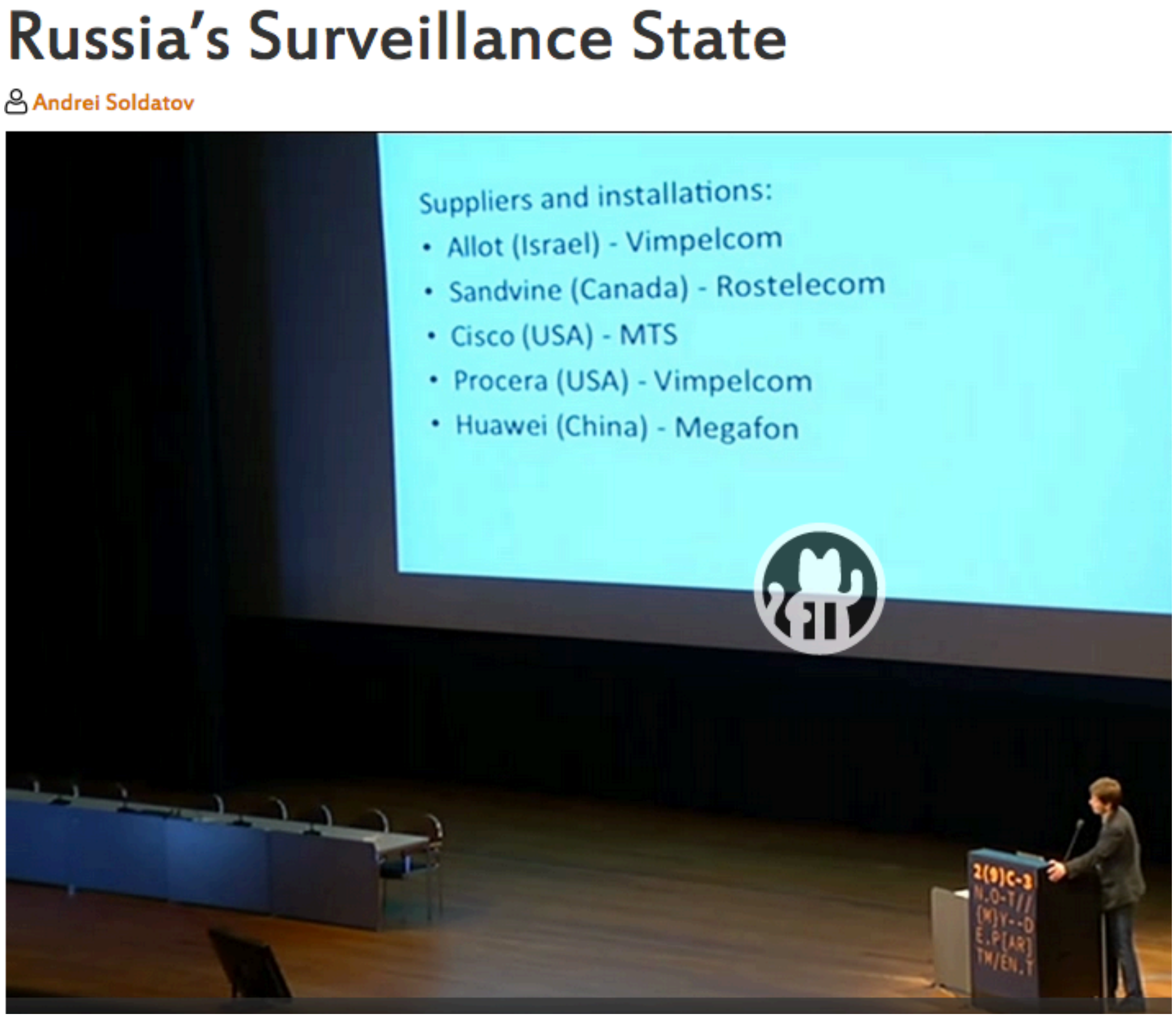
2012- 29C3 - Not my department

The ultimate Galaksija talk

Everything about a Yugoslavian microcomputer halfway between a TRS-80 and a ZX 80



2012- 29C3 - Not my department



Russia’s Surveillance State

Andrei Soldatov

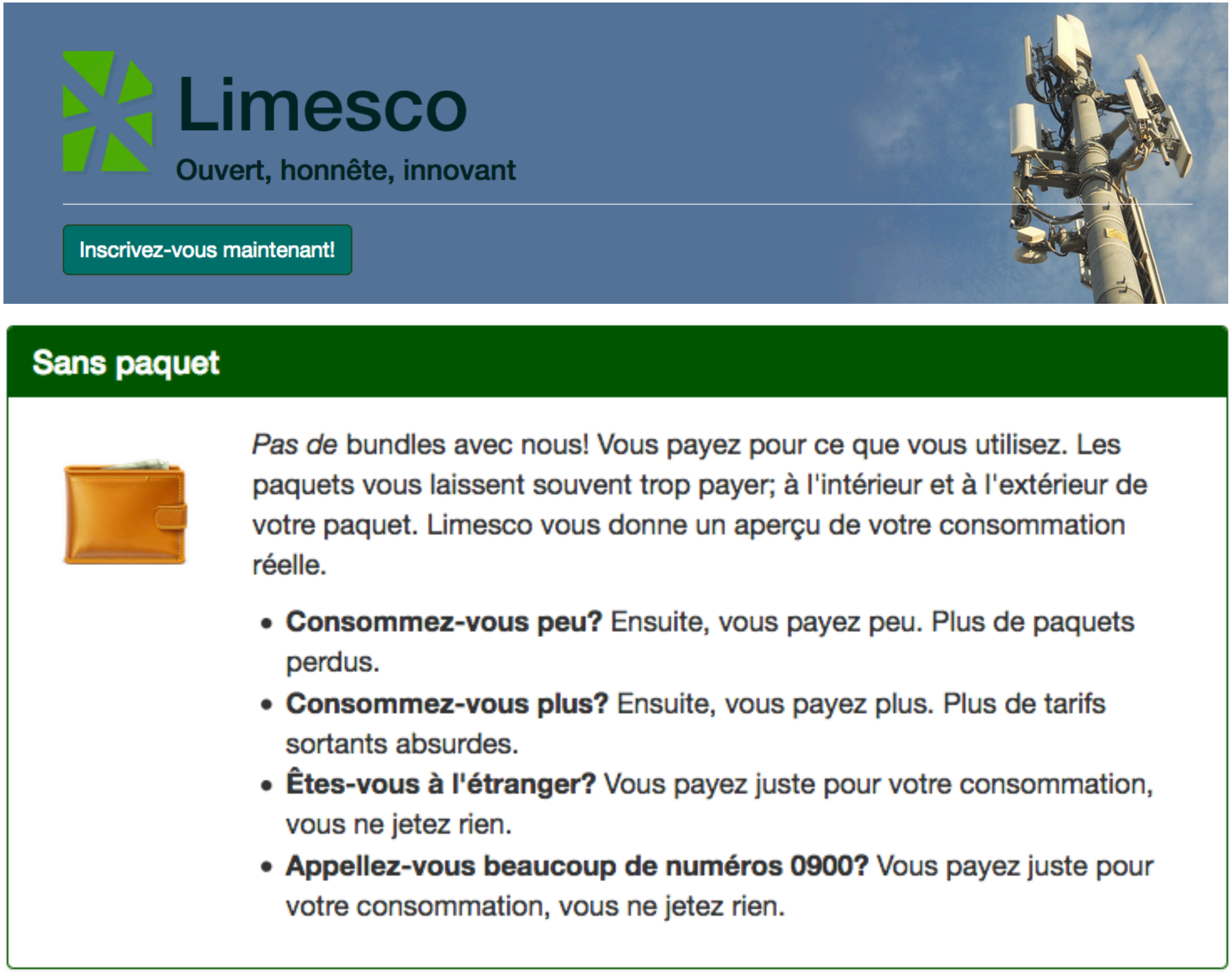
Suppliers and installations:

- Allot (Israel) - Vimpelcom
- Sandvine (Canada) - Rostelecom
- Cisco (USA) - MTS
- Procera (USA) - Vimpelcom
- Huawei (China) - Megafon

Privacy International, Agentura.Ru, the Russian secret services watchdog, and Citizen Lab have joined forces to launch a new project entitled 'Russia’s Surveillance State'.

The aims of the project are to undertake research and investigation into surveillance practices in Russia, including the trade in and use of surveillance technologies, and to publicise research and investigative findings to improve national and international awareness of surveillance and secrecy practices in Russia.

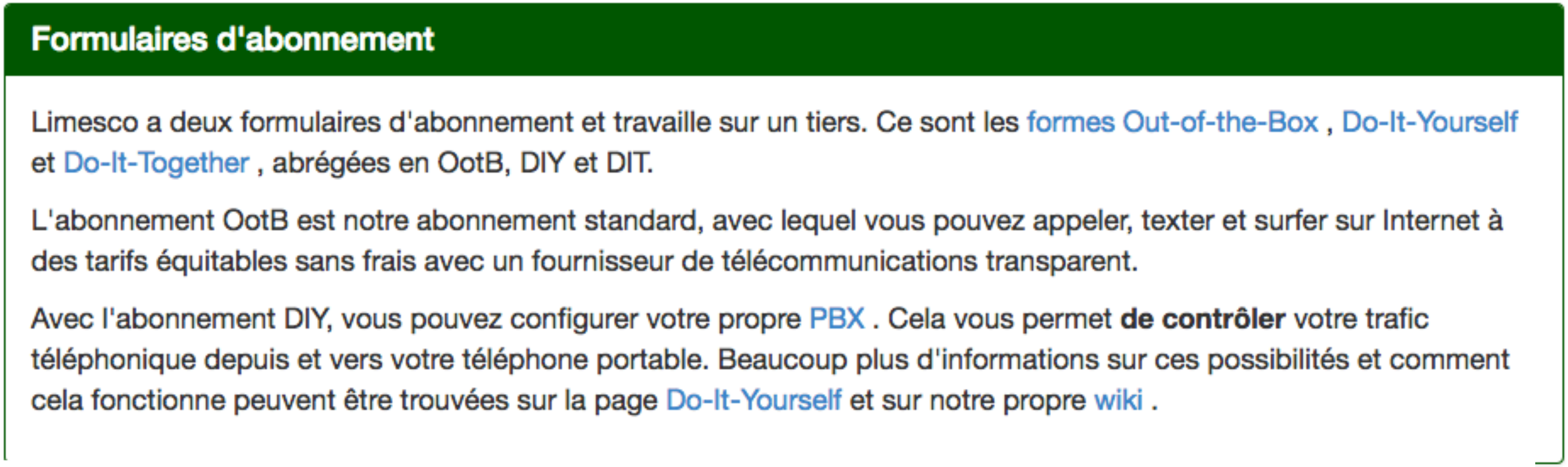
Ouverture de Limesco



Sans paquet

Pas de bundles avec nous! Vous payez pour ce que vous utilisez. Les paquets vous laissent souvent trop payer; à l'intérieur et à l'extérieur de votre paquet. Limesco vous donne un aperçu de votre consommation réelle.

- **Consommez-vous peu?** Ensuite, vous payez peu. Plus de paquets perdus.
- **Consommez-vous plus?** Ensuite, vous payez plus. Plus de tarifs sortants absurdes.
- **Êtes-vous à l'étranger?** Vous payez juste pour votre consommation, vous ne jetez rien.
- **Appellez-vous beaucoup de numéros 0900?** Vous payez juste pour votre consommation, vous ne jetez rien.

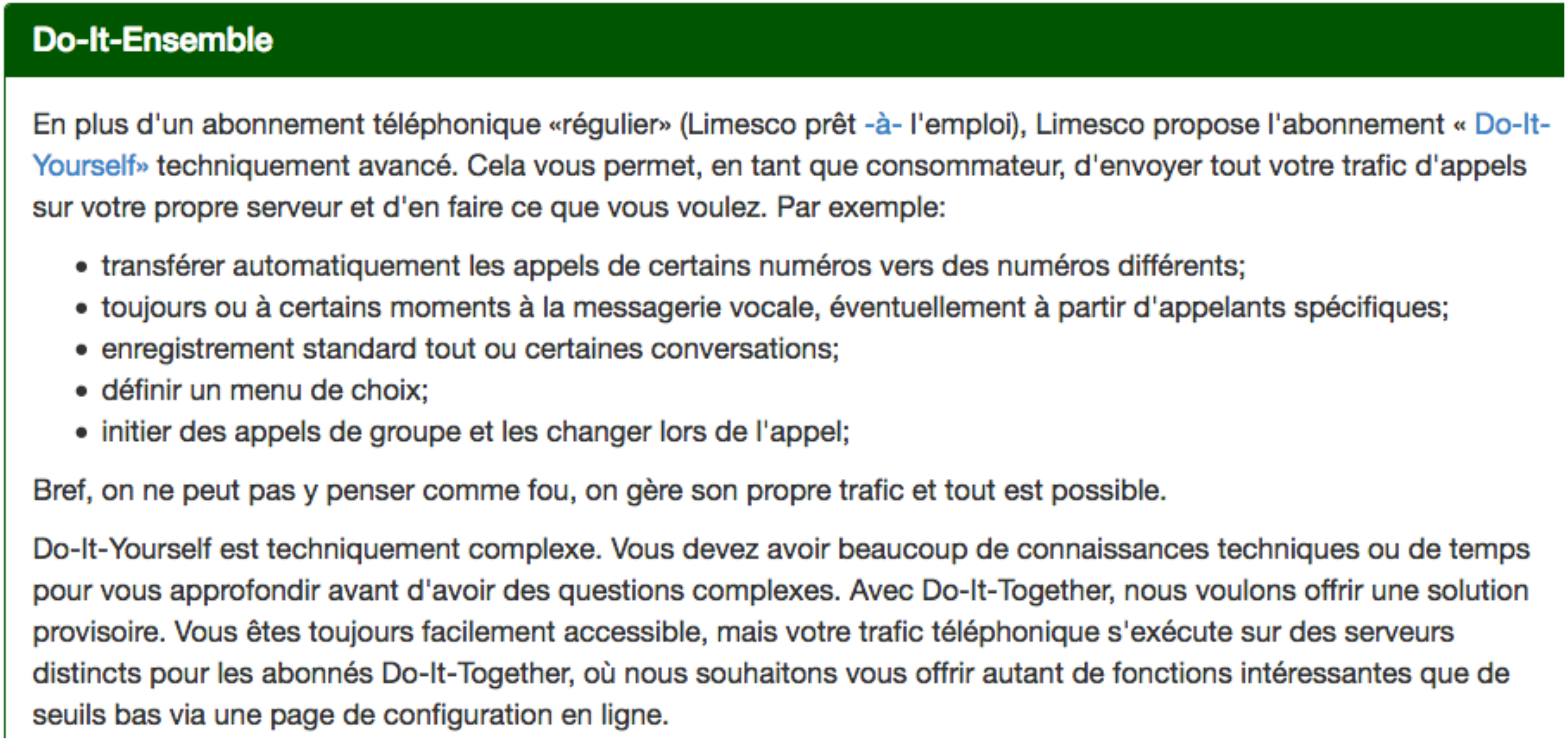


Formulaires d'abonnement

Limesco a deux formulaires d'abonnement et travaille sur un tiers. Ce sont les formes Out-of-the-Box , Do-It-Yourself et Do-It-Together , abrégées en OotB, DIY et DIT.

L'abonnement OotB est notre abonnement standard, avec lequel vous pouvez appeler, texter et surfer sur Internet à des tarifs équitables sans frais avec un fournisseur de télécommunications transparent.

Avec l'abonnement DIY, vous pouvez configurer votre propre PBX . Cela vous permet **de contrôler** votre trafic téléphonique depuis et vers votre téléphone portable. Beaucoup plus d'informations sur ces possibilités et comment cela fonctionne peuvent être trouvées sur la page Do-It-Yourself et sur notre propre wiki .



Do-It-Ensemble

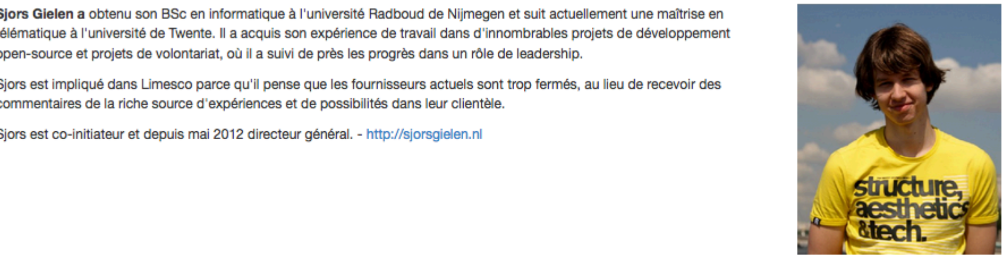
En plus d'un abonnement téléphonique «régulier» (Limesco prêt -à- l'emploi), Limesco propose l'abonnement « Do-It-Yourself» techniquement avancé. Cela vous permet, en tant que consommateur, d'envoyer tout votre trafic d'appels sur votre propre serveur et d'en faire ce que vous voulez. Par exemple:

- transférer automatiquement les appels de certains numéros vers des numéros différents;
- toujours ou à certains moments à la messagerie vocale, éventuellement à partir d'appelants spécifiques;
- enregistrement standard tout ou certaines conversations;
- définir un menu de choix;
- initier des appels de groupe et les changer lors de l'appel;

Bref, on ne peut pas y penser comme fou, on gère son propre trafic et tout est possible.

Do-It-Yourself est techniquement complexe. Vous devez avoir beaucoup de connaissances techniques ou de temps pour vous approfondir avant d'avoir des questions complexes. Avec Do-It-Together, nous voulons offrir une solution provisoire. Vous êtes toujours facilement accessible, mais votre trafic téléphonique s'exécute sur des serveurs distincts pour les abonnés Do-It-Together, où nous souhaitons vous offrir autant de fonctions intéressantes que de seuils bas via une page de configuration en ligne.

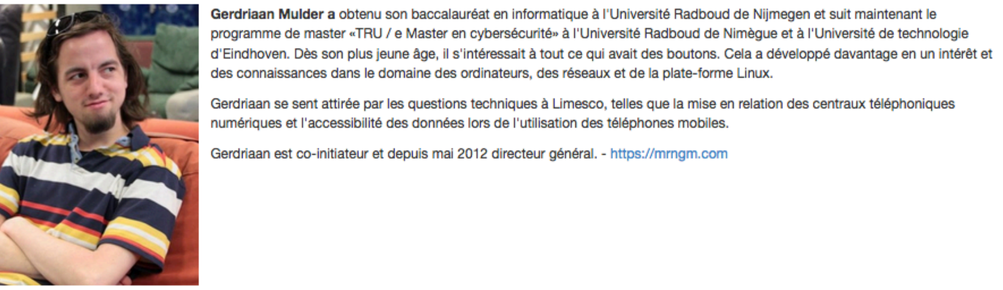
2012- 29C3 - Not my department



Sjors Gielen a obtenu son BSc en informatique à l'université Radboud de Nijmegen et suit actuellement une maîtrise en élématique à l'université de Twente. Il a acquis son expérience de travail dans d'innombrables projets de développement open-source et projets de volontariat, où il a suivi de près les progrès dans un rôle de leadership.

Sjors est impliqué dans Limesco parce qu'il pense que les fournisseurs actuels sont trop fermés, au lieu de recevoir des commentaires de la riche source d'expériences et de possibilités dans leur clientèle.

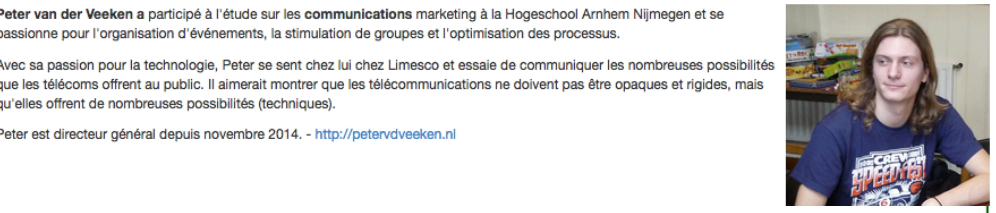
Sjors est co-initiateur et depuis mai 2012 directeur général. - http://sjorsgielen.nl



Gerdriaan Mulder a obtenu son baccalauréat en informatique à l'Université Radboud de Nijmegen et suit maintenant le programme de master «TRU / e Master en cybersécurité» à l'Université Radboud de Nimègue et à l'Université de technologie d'Eindhoven. Dès son plus jeune âge, il s'intéressait à tout ce qui avait des boutons. Cela a développé davantage en un intérêt et des connaissances dans le domaine des ordinateurs, des réseaux et de la plate-forme Linux.

Gerdriaan se sent attirée par les questions techniques à Limesco, telles que la mise en relation des centraux téléphoniques numériques et l'accessibilité des données lors de l'utilisation des téléphones mobiles.

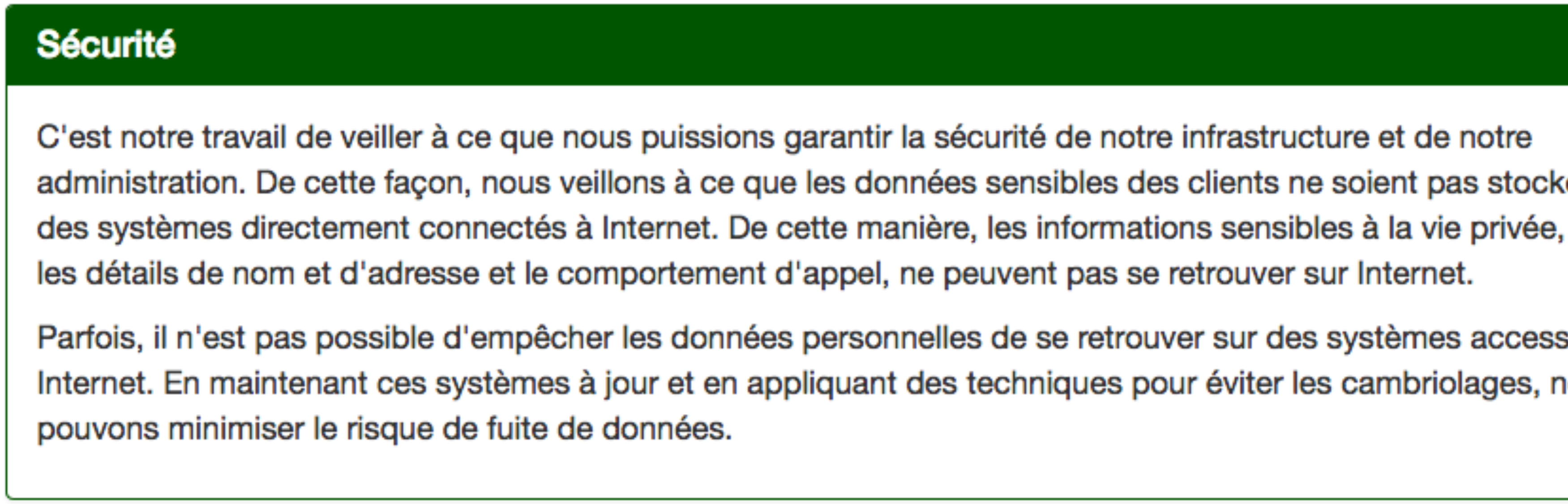
Gerdriaan est co-initiateur et depuis mai 2012 directeur général. - https://mrngm.com



Peter van der Veeken a participé à l'étude sur les **communications** marketing à la Hogeschool Arnhem Nijmegen et se passionne pour l'organisation d'événements, la stimulation de groupes et l'optimisation des processus.

Avec sa passion pour la technologie, Peter se sent chez lui chez Limesco et essaie de communiquer les nombreuses possibilités que les télécoms offrent au public. Il aimerait montrer que les télécommunications ne doivent pas être opaques et rigides, mais qu'elles offrent de nombreuses possibilités (techniques).

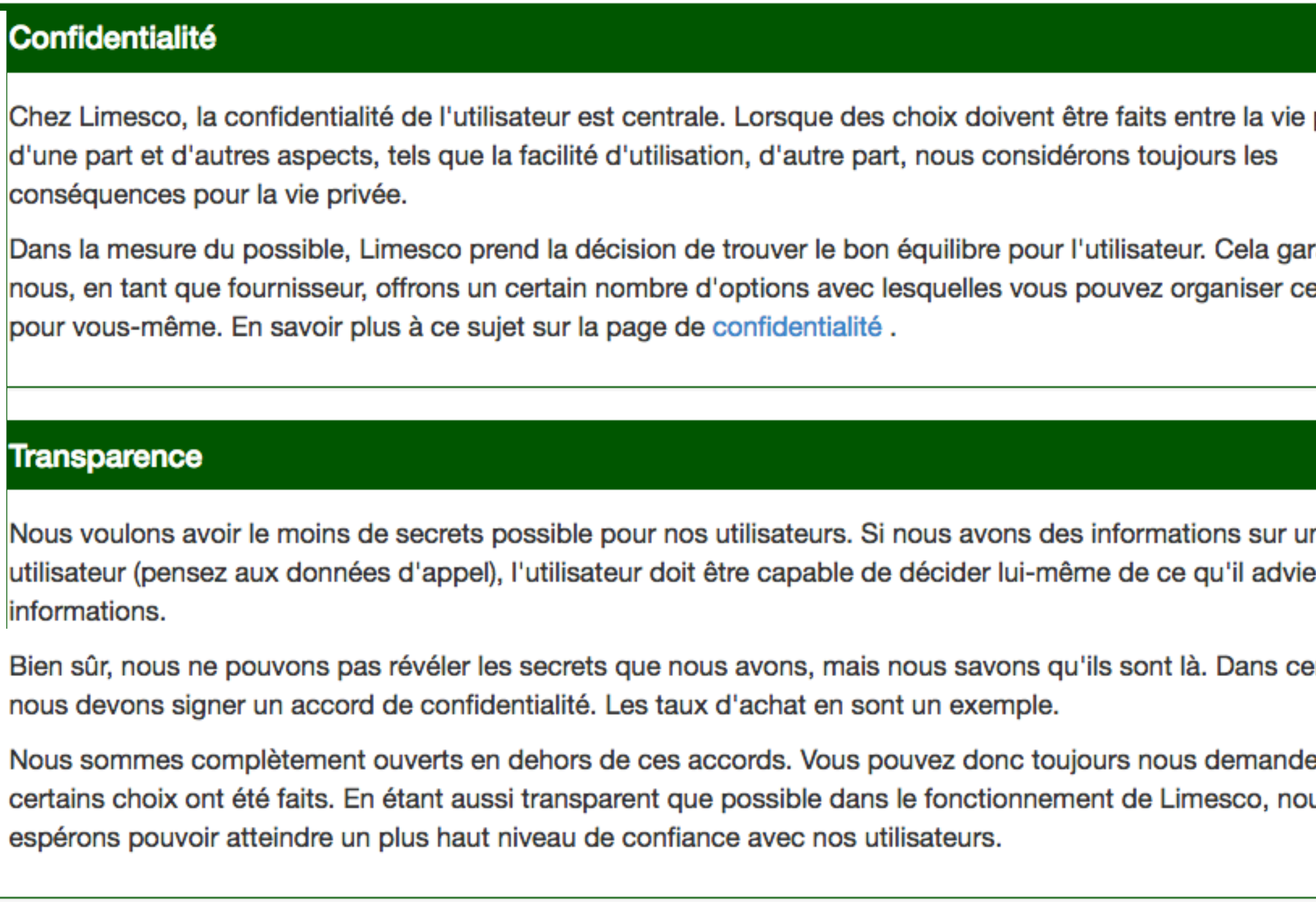
Peter est directeur général depuis novembre 2014. - http://petervdveeken.nl



Sécurité

C'est notre travail de veiller à ce que nous puissions garantir la sécurité de notre infrastructure et de notre administration. De cette façon, nous veillons à ce que les données sensibles des clients ne soient pas stock des systèmes directement connectés à Internet. De cette manière, les informations sensibles à la vie privée, les détails de nom et d'adresse et le comportement d'appel, ne peuvent pas se retrouver sur Internet.

Parfois, il n'est pas possible d'empêcher les données personnelles de se retrouver sur des systèmes access Internet. En maintenant ces systèmes à jour et en appliquant des techniques pour éviter les cambriolages, n pouvons minimiser le risque de fuite de données.



Confidentialité

Chez Limesco, la confidentialité de l'utilisateur est centrale. Lorsque des choix doivent être faits entre la vie d'une part et d'autres aspects, tels que la facilité d'utilisation, d'autre part, nous considérons toujours les conséquences pour la vie privée.

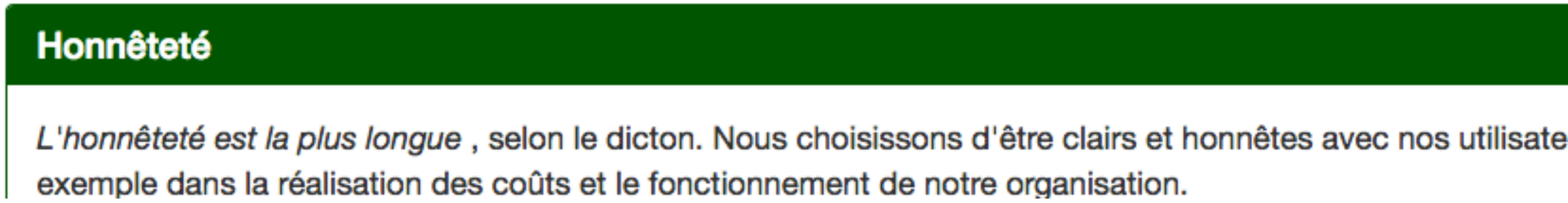
Dans la mesure du possible, Limesco prend la décision de trouver le bon équilibre pour l'utilisateur. Cela gar nous, en tant que fournisseur, offrons un certain nombre d'options avec lesquelles vous pouvez organiser ce pour vous-même. En savoir plus à ce sujet sur la page de confidentialité .

Transparence

Nous voulons avoir le moins de secrets possible pour nos utilisateurs. Si nous avons des informations sur ur utilisateur (pensez aux données d'appel), l'utilisateur doit être capable de décider lui-même de ce qu'il advie informations.

Bien sûr, nous ne pouvons pas révéler les secrets que nous avons, mais nous savons qu'ils sont là. Dans ce nous devons signer un accord de confidentialité. Les taux d'achat en sont un exemple.

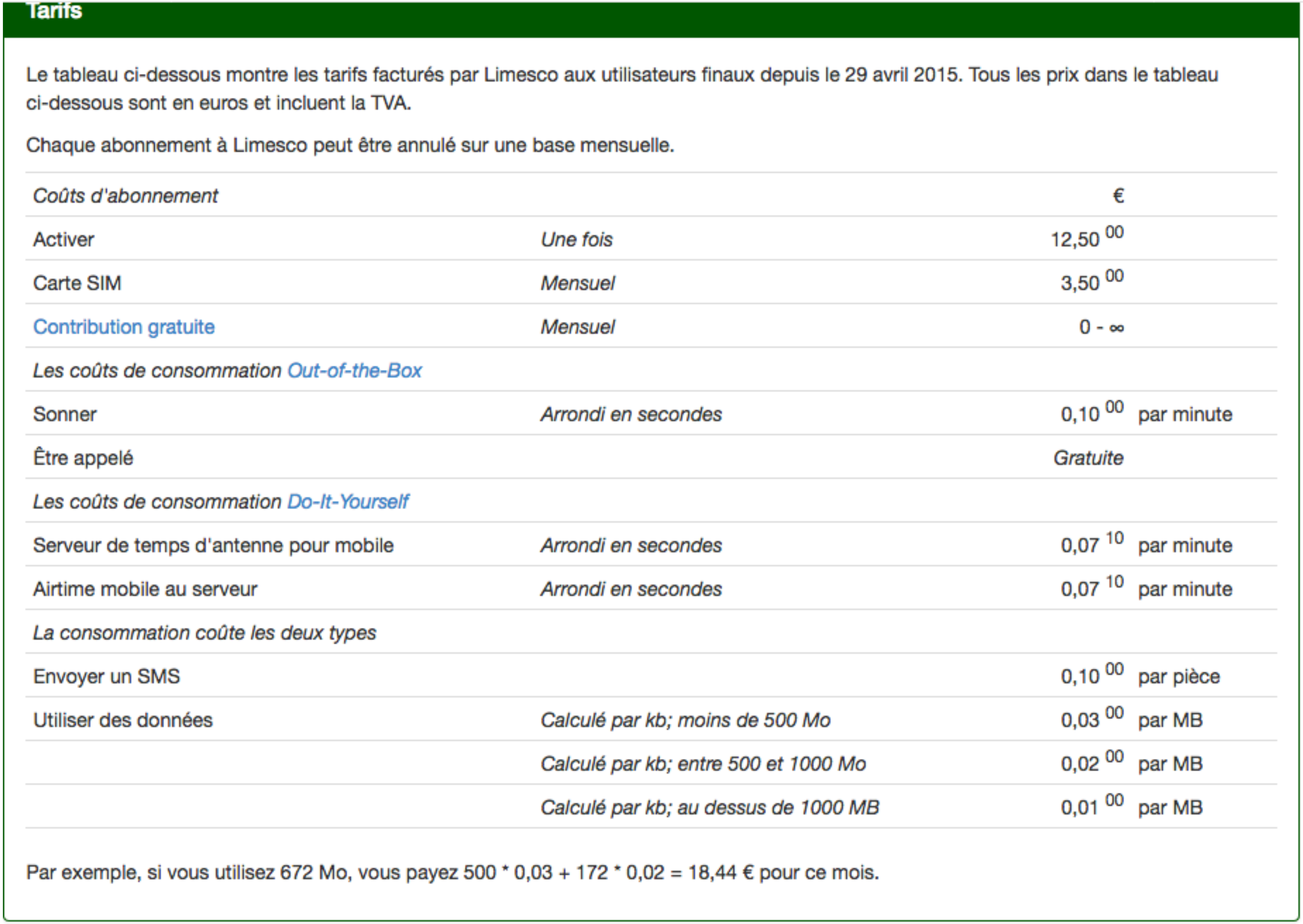
Nous sommes complètement ouverts en dehors de ces accords. Vous pouvez donc toujours nous demande certains choix ont été faits. En étant aussi transparent que possible dans le fonctionnement de Limesco, nou espérons pouvoir atteindre un plus haut niveau de confiance avec nos utilisateurs.



Honnêteté

L'honnêteté est la plus longue , selon le dicton. Nous choisissons d'être clairs et honnêtes avec nos utilisate exemple dans la réalisation des coûts et le fonctionnement de notre organisation.

2012- 29C3 - Not my department



Tarifs

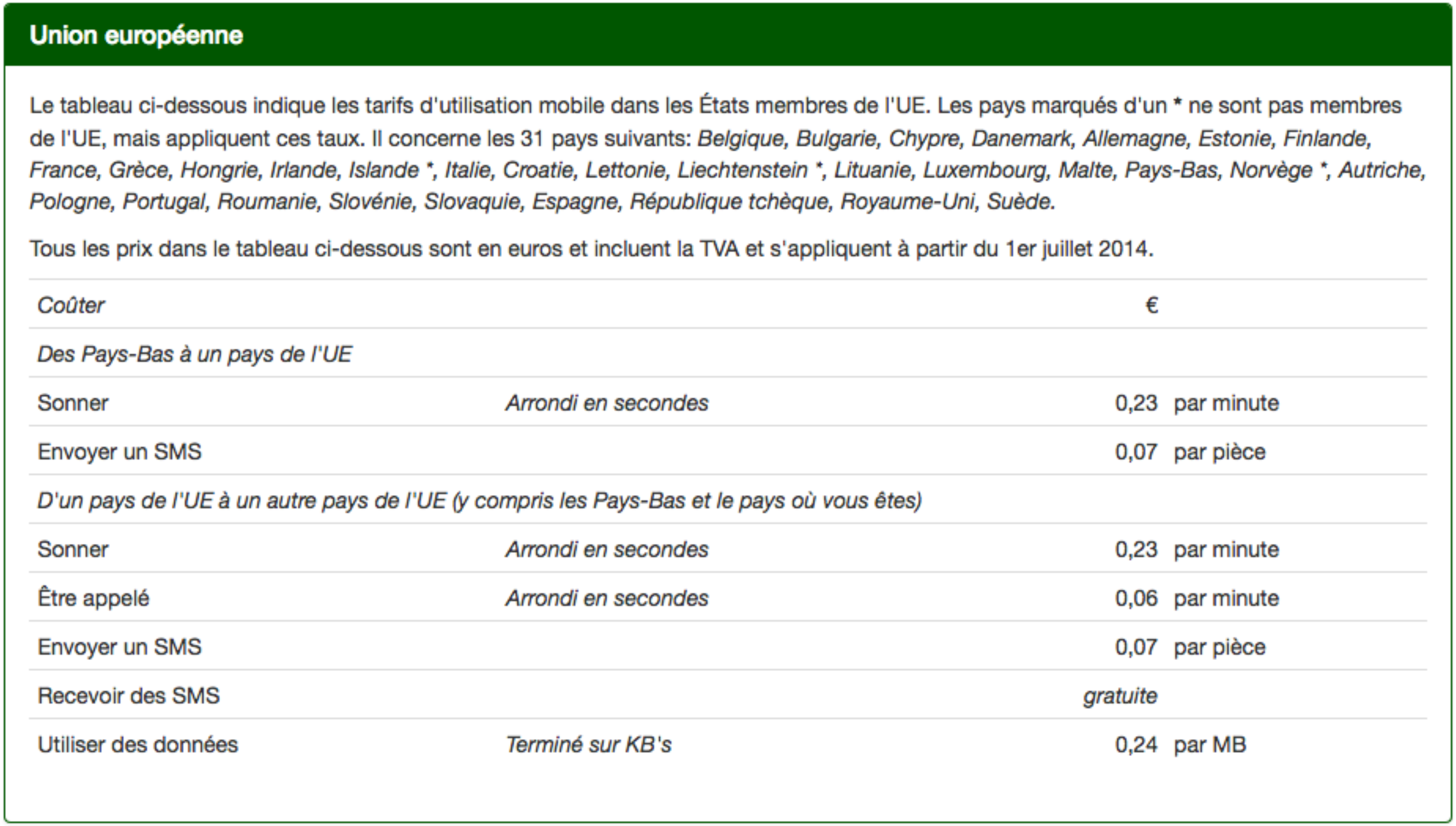
Le tableau ci-dessous montre les tarifs facturés par Limesco aux utilisateurs finaux depuis le 29 avril 2015. Tous les prix dans le tableau ci-dessous sont en euros et incluent la TVA.

Chaque abonnement à Limesco peut être annulé sur une base mensuelle.

Coûts d'abonnement		€	
Activer	*Une fois*	12,50 ^{00}	
Carte SIM	*Mensuel*	3,50 ^{00}	
Contribution gratuite	*Mensuel*	0 - ∞	
Les coûts de consommation Out-of-the-Box			
Sonner	*Arrondi en secondes*	0,10 ^{00}	par minute
Être appelé		*Gratuite*	
Les coûts de consommation Do-It-Yourself			
Serveur de temps d'antenne pour mobile	*Arrondi en secondes*	0,07 ^{10}	par minute
Airtime mobile au serveur	*Arrondi en secondes*	0,07 ^{10}	par minute
La consommation coûte les deux types			
Envoyer un SMS		0,10 ^{00}	par pièce
Utiliser des données	*Calculé par kb; moins de 500 Mo*	0,03 ^{00}	par MB
	Calculé par kb; entre 500 et 1000 Mo	0,02 ^{00}	par MB
	Calculé par kb; au dessus de 1000 MB	0,01 ^{00}	par MB

Par exemple, si vous utilisez 672 Mo, vous payez 500 * 0,03 + 172 * 0,02 = 18,44 € pour ce mois.

2012- 29C3 - Not my department

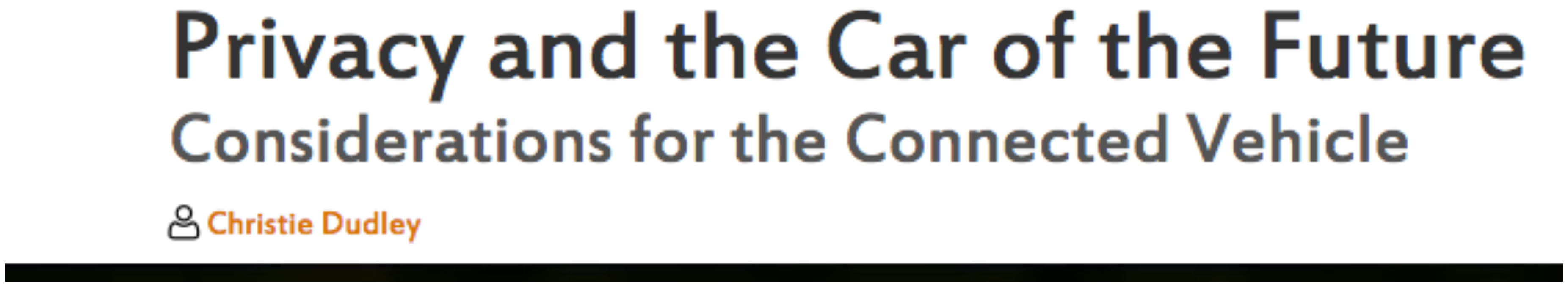


Union européenne

Le tableau ci-dessous indique les tarifs d'utilisation mobile dans les États membres de l'UE. Les pays marqués d'un * ne sont pas membres de l'UE, mais appliquent ces taux. Il concerne les 31 pays suivants: *Belgique, Bulgarie, Chypre, Danemark, Allemagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande *, Italie, Croatie, Lettonie, Liechtenstein *, Lituanie, Luxembourg, Malte, Pays-Bas, Norvège *, Autriche, Pologne, Portugal, Roumanie, Slovénie, Slovaquie, Espagne, République tchèque, Royaume-Uni, Suède.*

Tous les prix dans le tableau ci-dessous sont en euros et incluent la TVA et s'appliquent à partir du 1er juillet 2014.

Coûter		€	
Des Pays-Bas à un pays de l'UE			
Sonner	*Arrondi en secondes*	0,23	par minute
Envoyer un SMS		0,07	par pièce
D'un pays de l'UE à un autre pays de l'UE (y compris les Pays-Bas et le pays où vous êtes)			
Sonner	*Arrondi en secondes*	0,23	par minute
Être appelé	*Arrondi en secondes*	0,06	par minute
Envoyer un SMS		0,07	par pièce
Recevoir des SMS		*gratuite*	
Utiliser des données	*Terminé sur KB's*	0,24	par MB

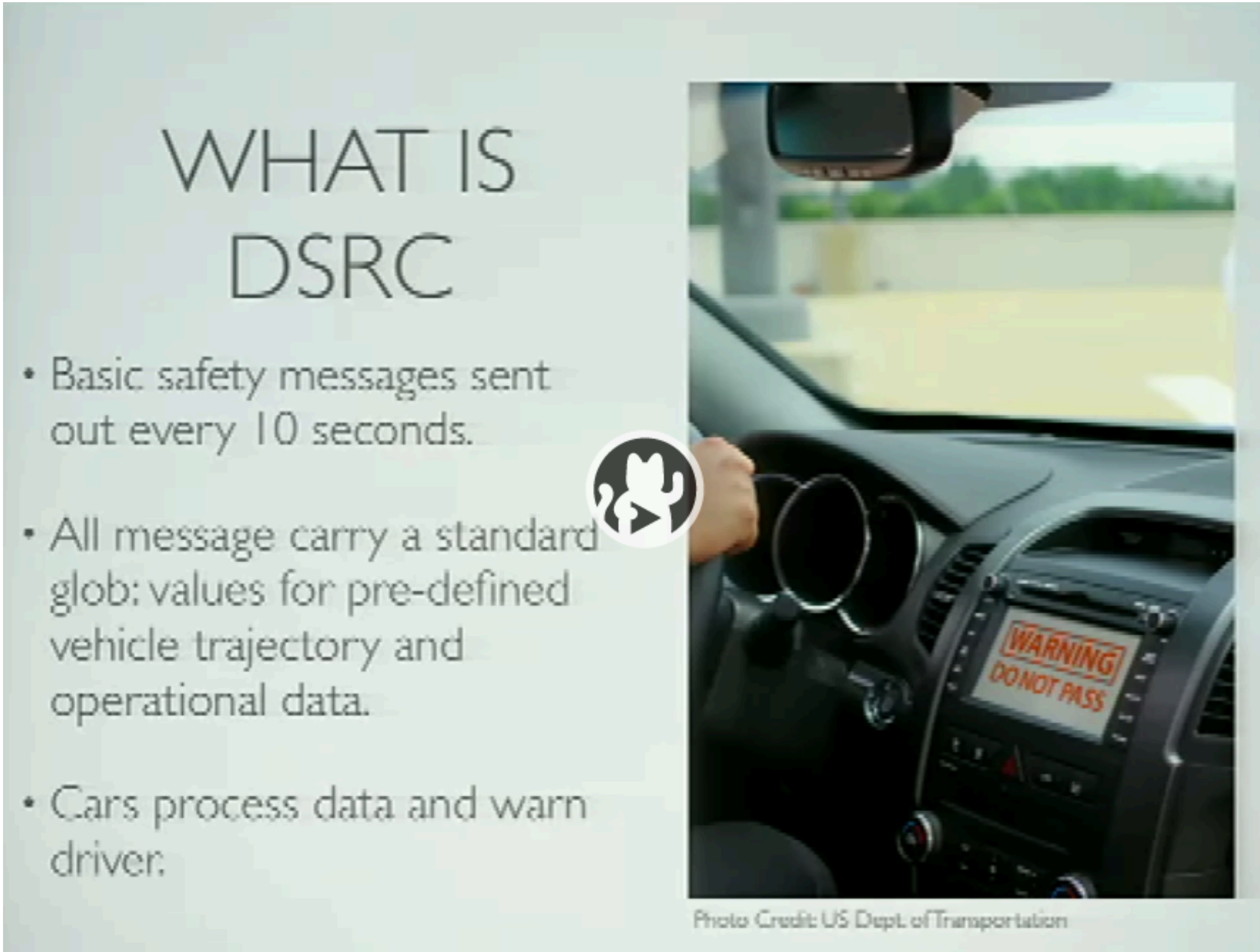


Privacy and the Car of the Future

Considerations for the Connected Vehicle

Christie Dudley

To date, remote vehicle communications have provided little in the way of privacy. Much information and misinformation has been spread on what the system is and can do, especially within the information security community. The recent field trial in the US of a connected vehicle infrastructure raises the level of concern amongst all who are aware of existing privacy issues.

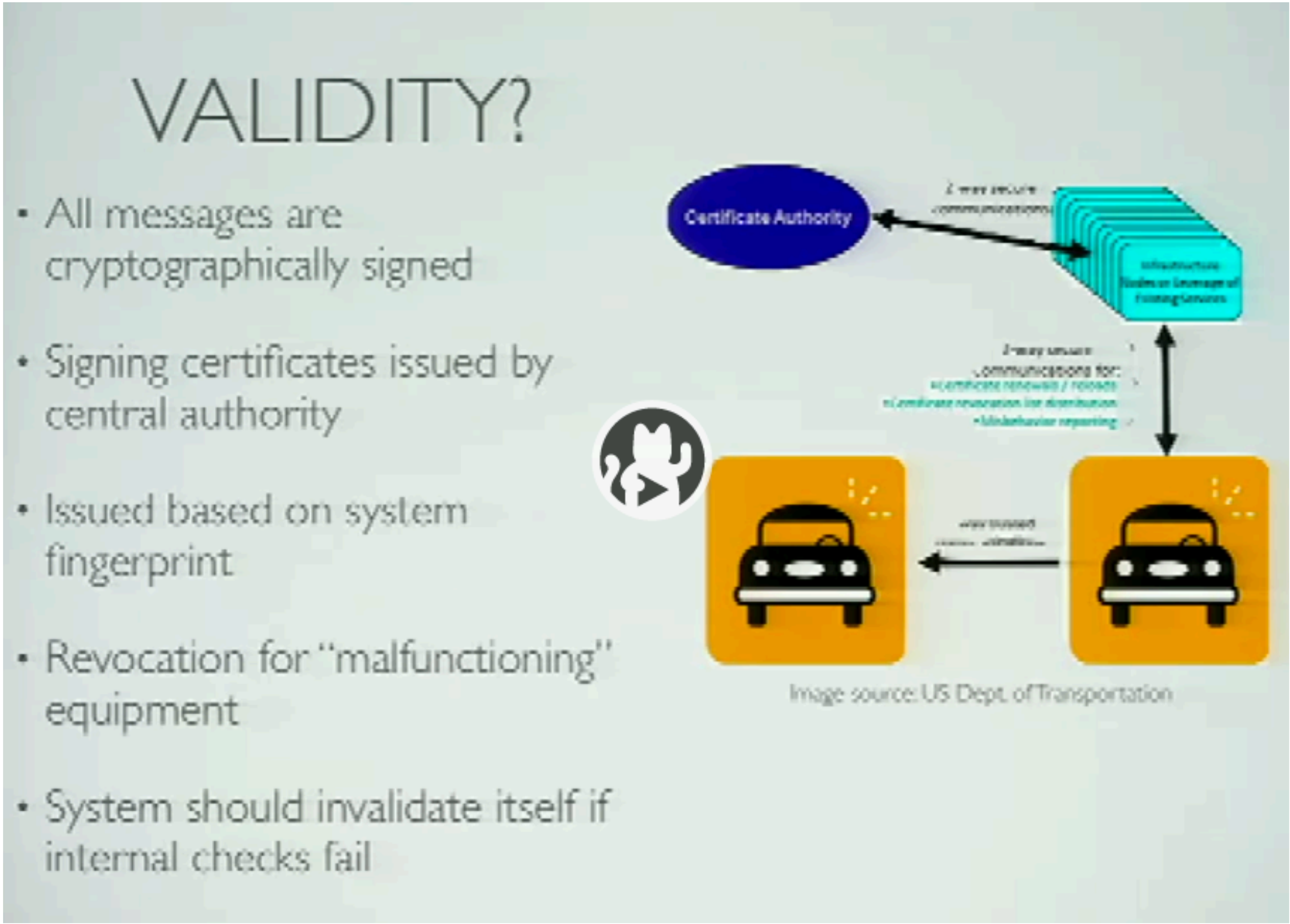


WHAT IS DSRC

- Basic safety messages sent out every 10 seconds.
- All message carry a standard glob: values for pre-defined vehicle trajectory and operational data.
- Cars process data and warn driver.

Photo Credit: US Dept. of Transportation

2012- 29C3 - Not my department



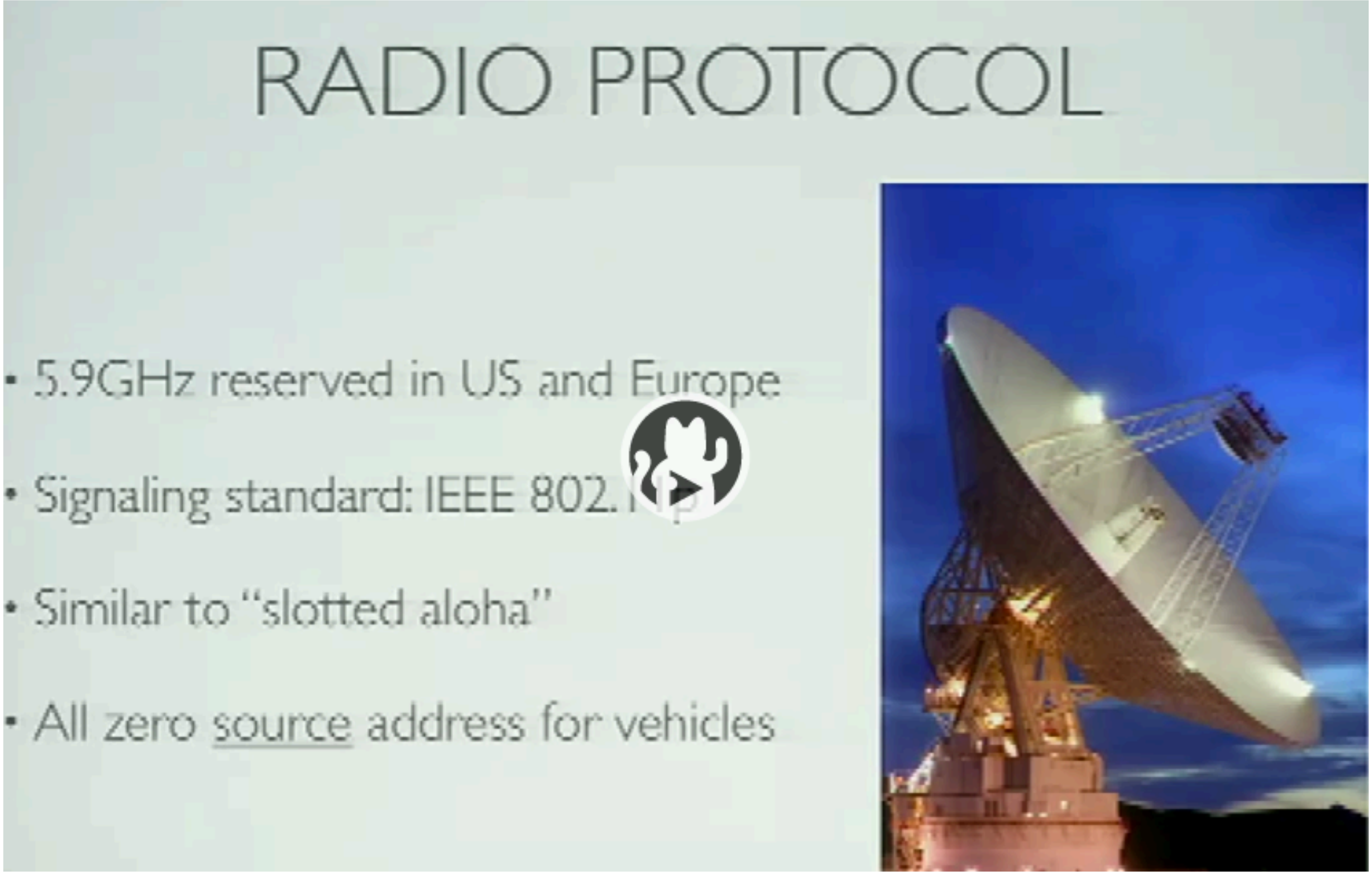
VALIDITY?

- All messages are cryptographically signed
- Signing certificates issued by central authority
- Issued based on system fingerprint
- Revocation for "malfunctioning" equipment
- System should invalidate itself if internal checks fail

Certificate Authority
2-way secure communications
Infrastructure Nodes or Leverage of Existing Services
2-way secure communications for:
•Certificate renewals / reloads
•Certificate revocation list distribution
•Misbehavior reporting
way trusted communications

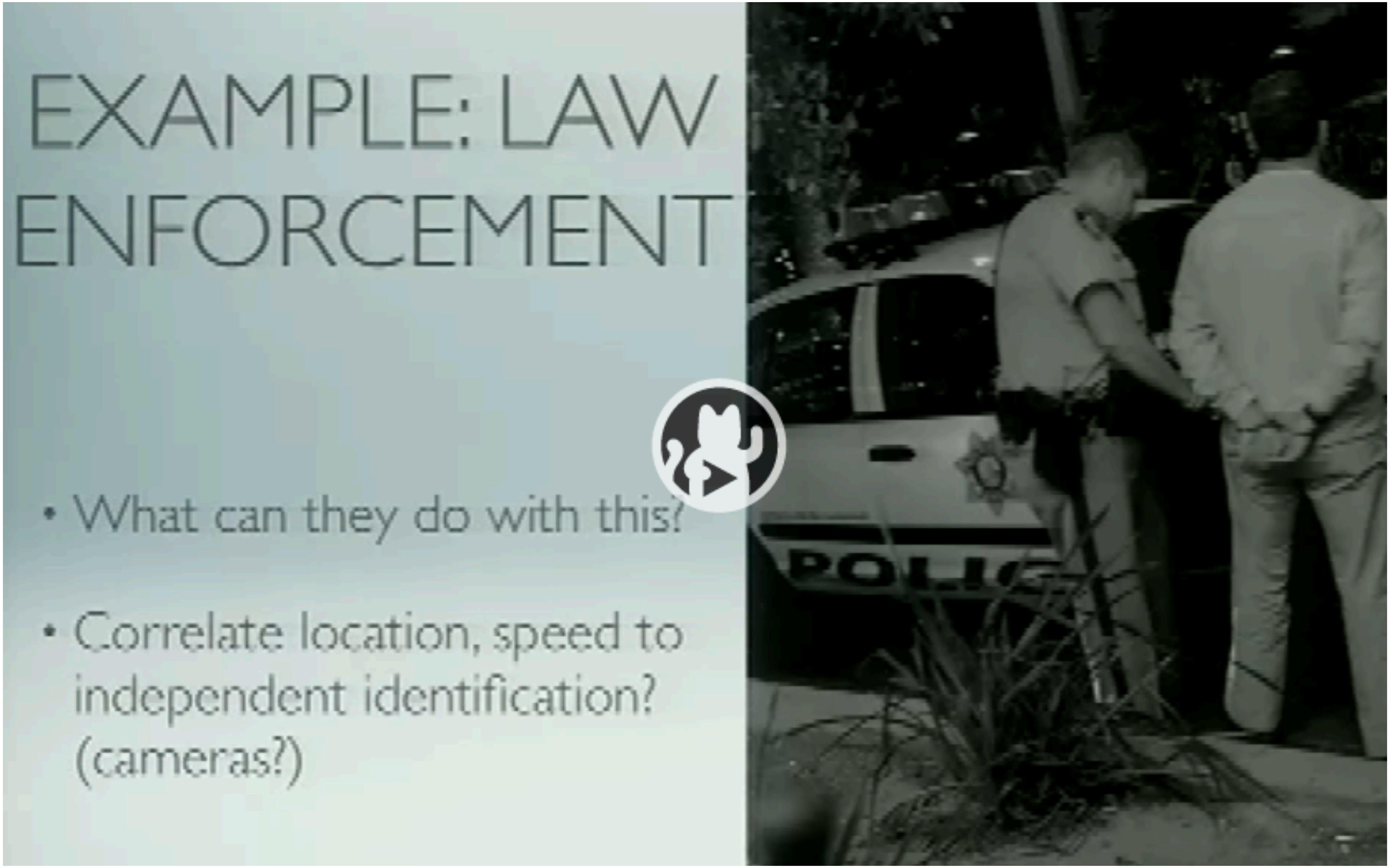
Image source: US Dept. of Transportation

2012- 29C3 - Not my department



RADIO PROTOCOL

- 5.9GHz reserved in US and Europe
- Signaling standard: IEEE 802.11p
- Similar to "slotted aloha"
- All zero source address for vehicles



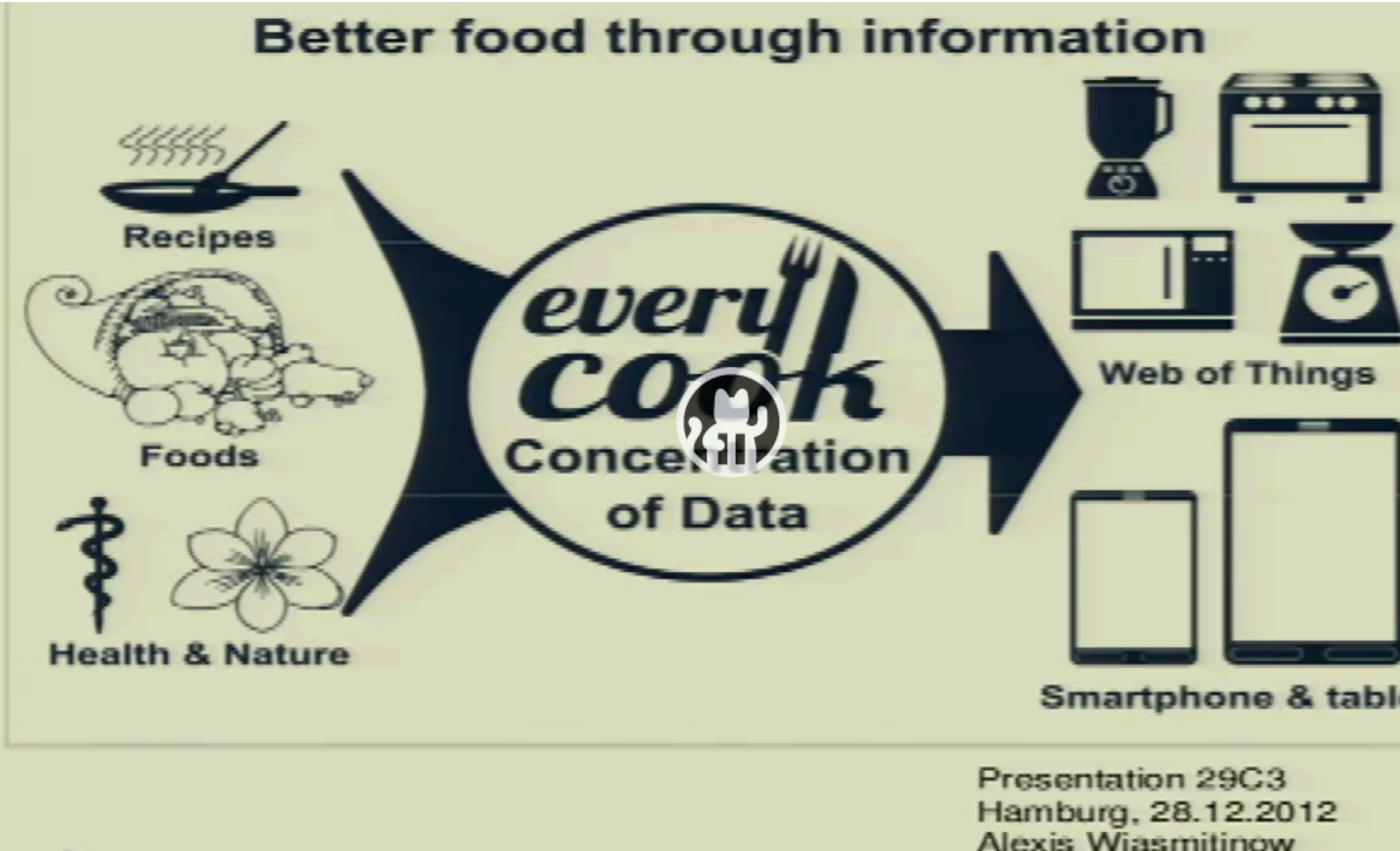
EXAMPLE: LAW ENFORCEMENT

- What can they do with this?
- Correlate location, speed to independent identification? (cameras?)

2012- 29C3 - Not my department

EveryCook

Cooking gets digital



Better food through information

Recipes

Foods

Health & Nature

every cook

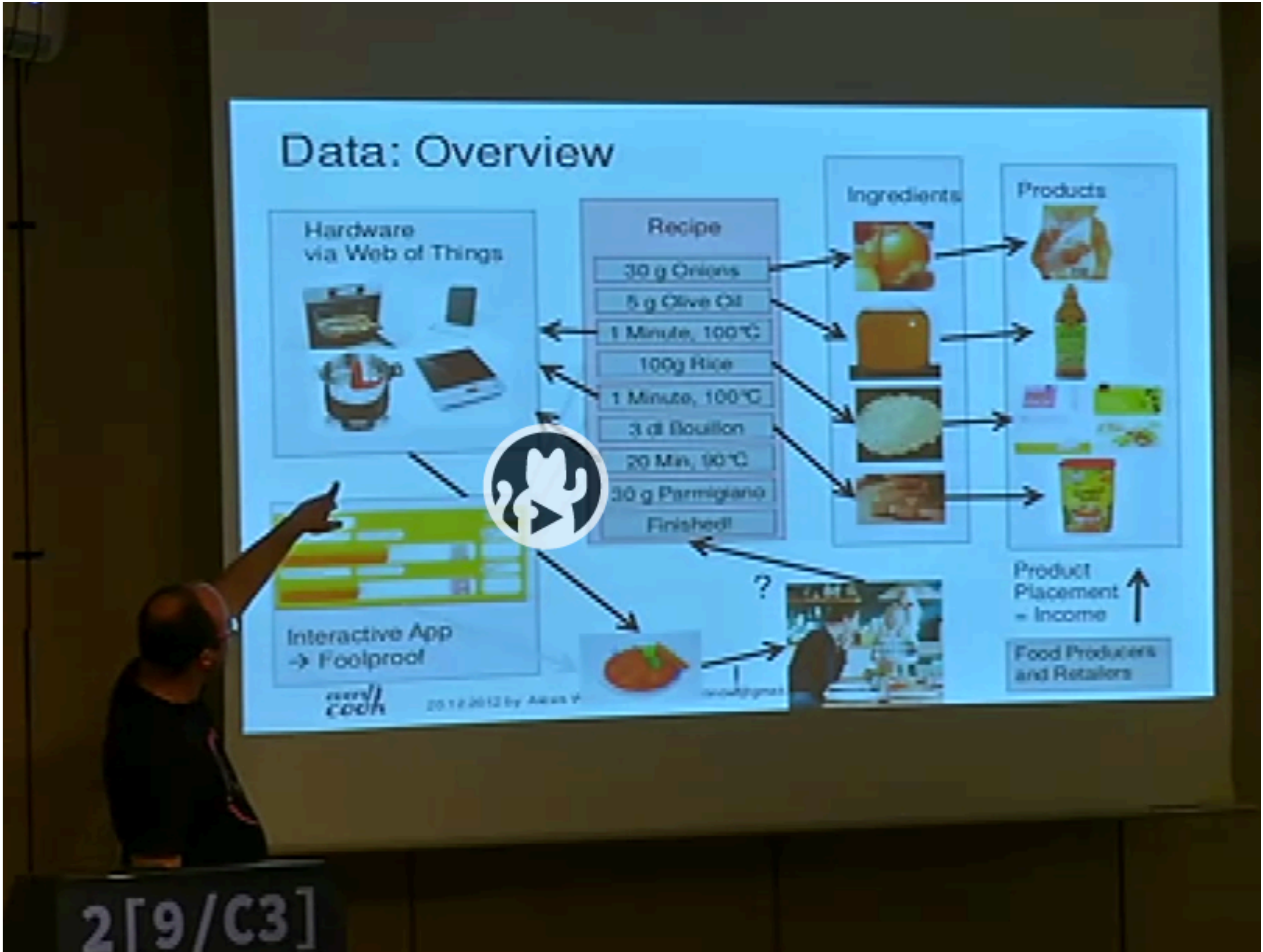
Concentration of Data

Web of Things

Smartphone & tabl

Presentation 29C3
Hamburg, 28.12.2012
Alexis Wiasmitinow

Data: Overview



Hardware
via Web of Things

Recipe

30 g Onions
5 g Olive Oil
1 Minute, 100°C
100g Rice
1 Minute, 100°C
3 dl Bouillon
20 Min, 90°C
30 g Parmigiano
Finished!

Ingredients

Products

Interactive App
-> Foolproof

?

Product
Placement
= Income

Food Producers
and Retailers

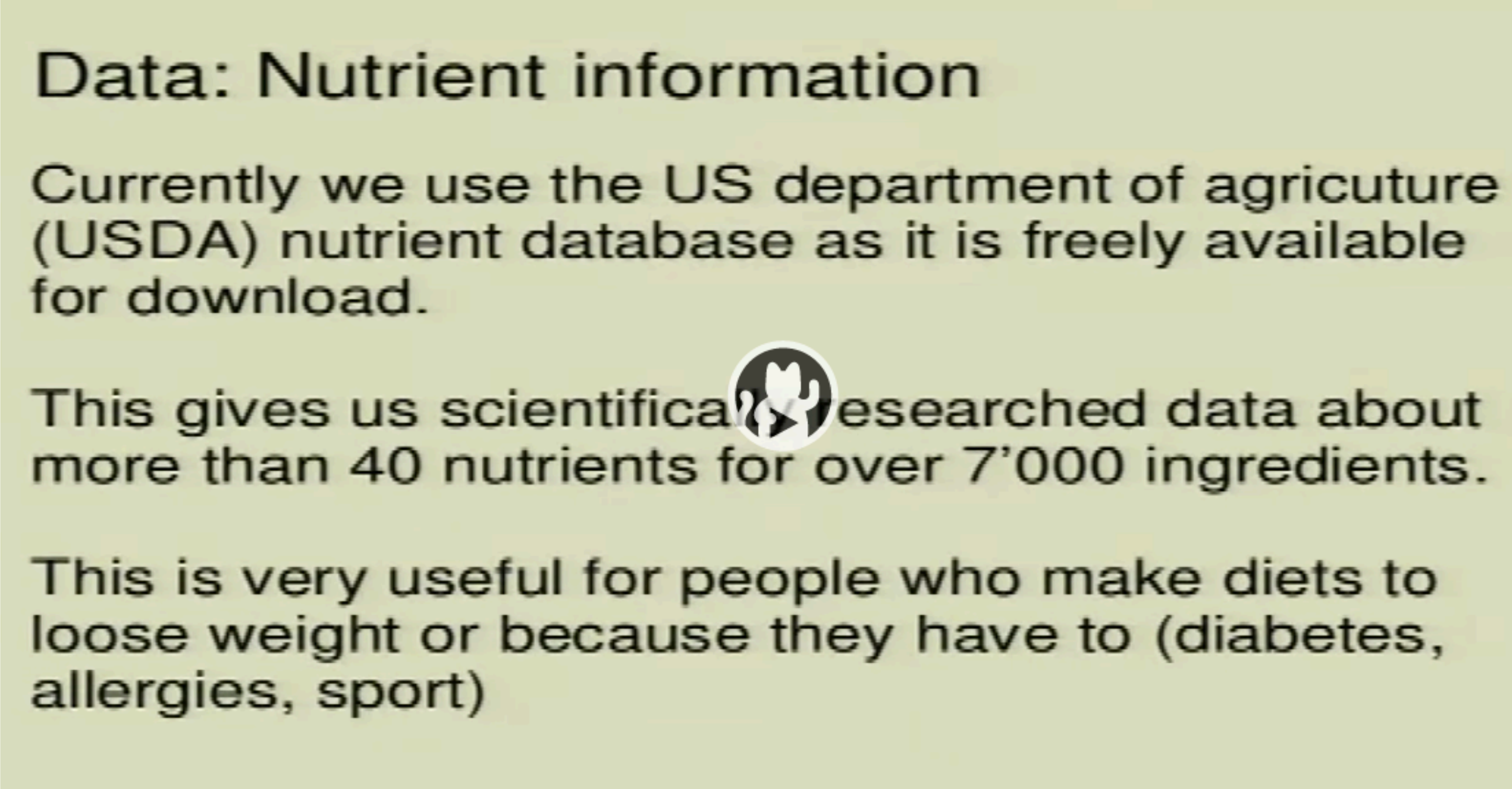
Opportunities: Hacking Competitors

Vorwerk Thermomix

Kuhn Rikon Duromatic Relax

Kenwood Cooking Chef

Philips Home Cooker

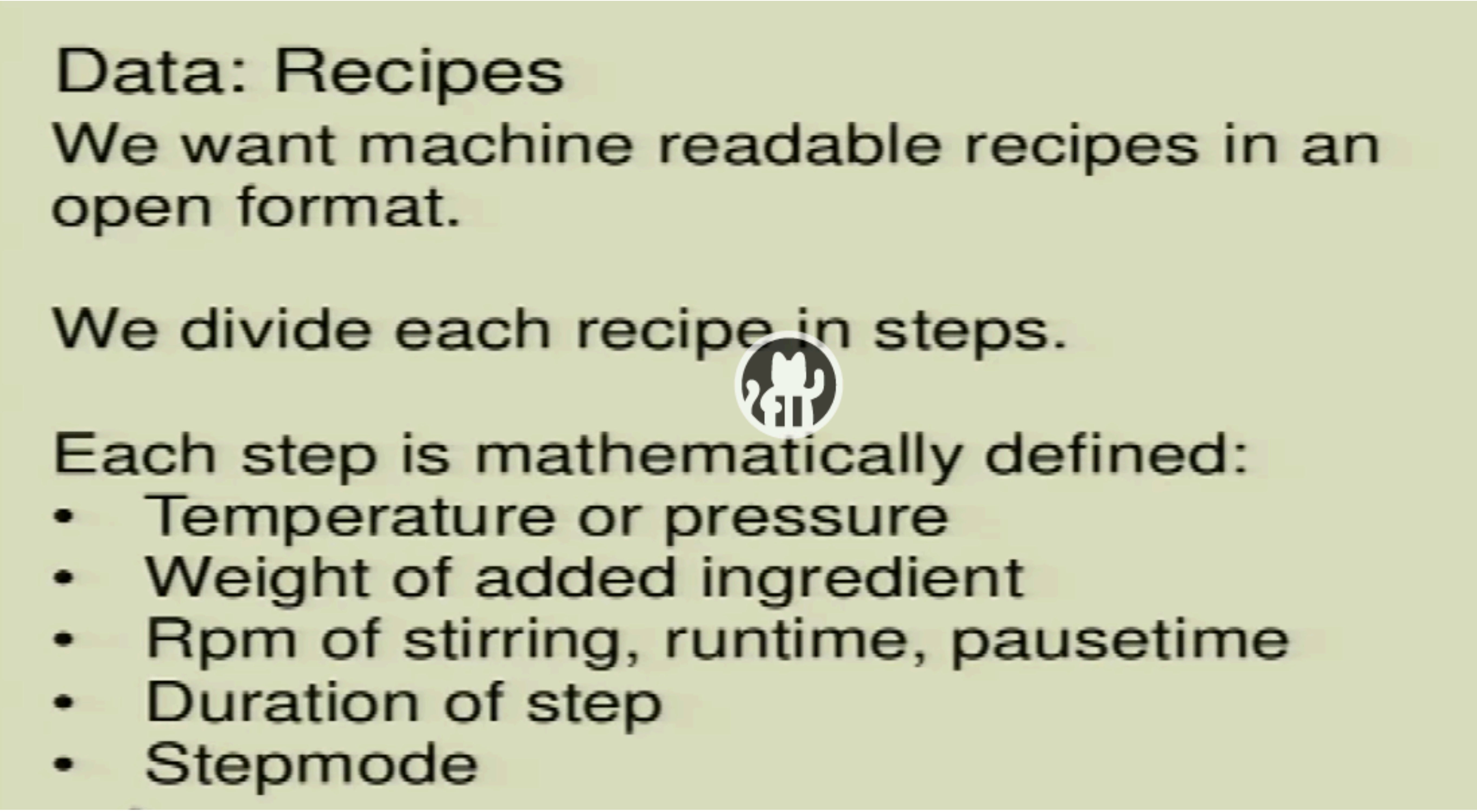


Data: Nutrient information

Currently we use the US department of agricuture (USDA) nutrient database as it is freely available for download.

This gives us scientifically researched data about more than 40 nutrients for over 7’000 ingredients.

This is very useful for people who make diets to loose weight or because they have to (diabetes, allergies, sport)



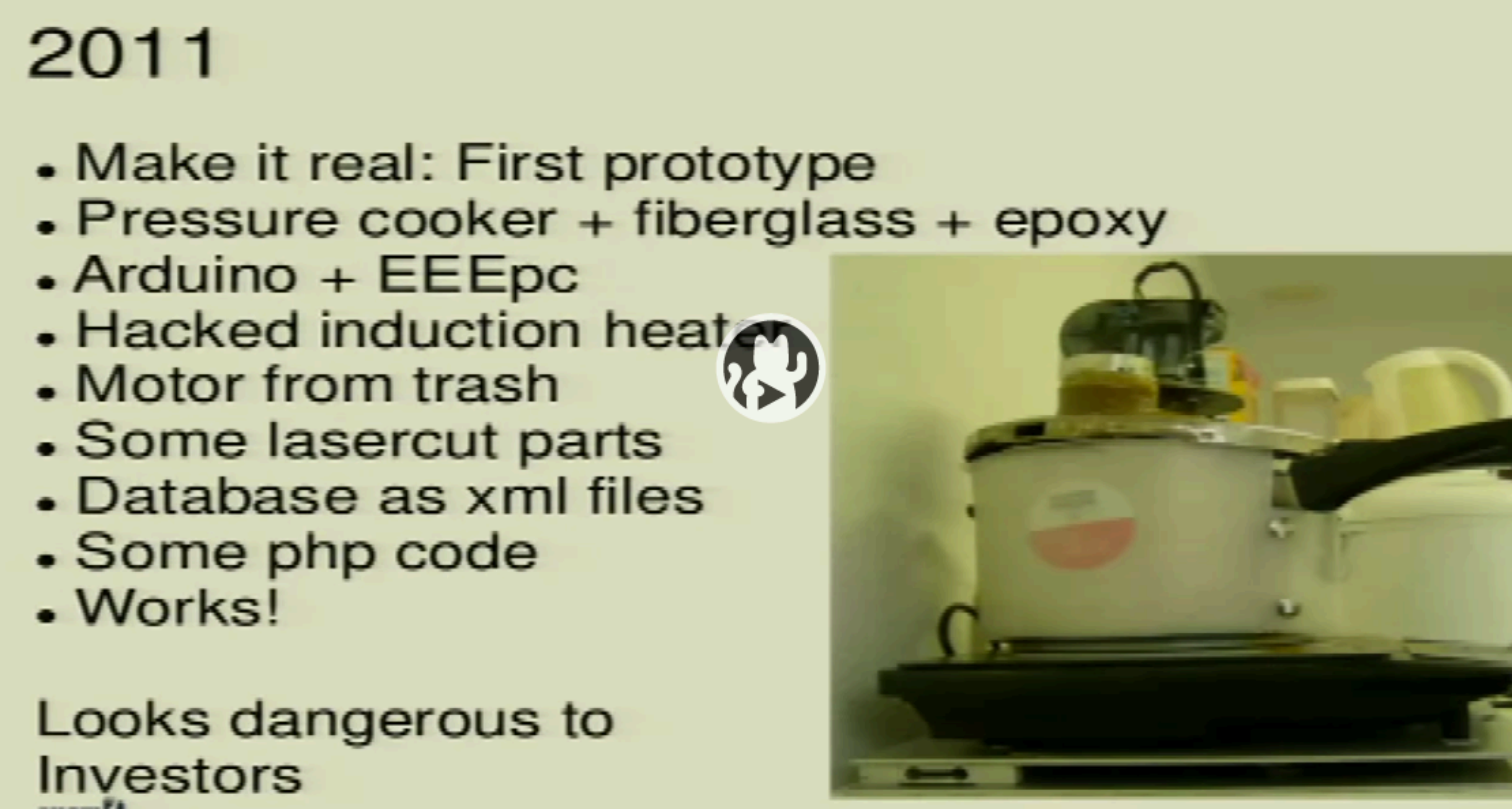
Data: Recipes

We want machine readable recipes in an open format.

We divide each recipe in steps.

Each step is mathematically defined:

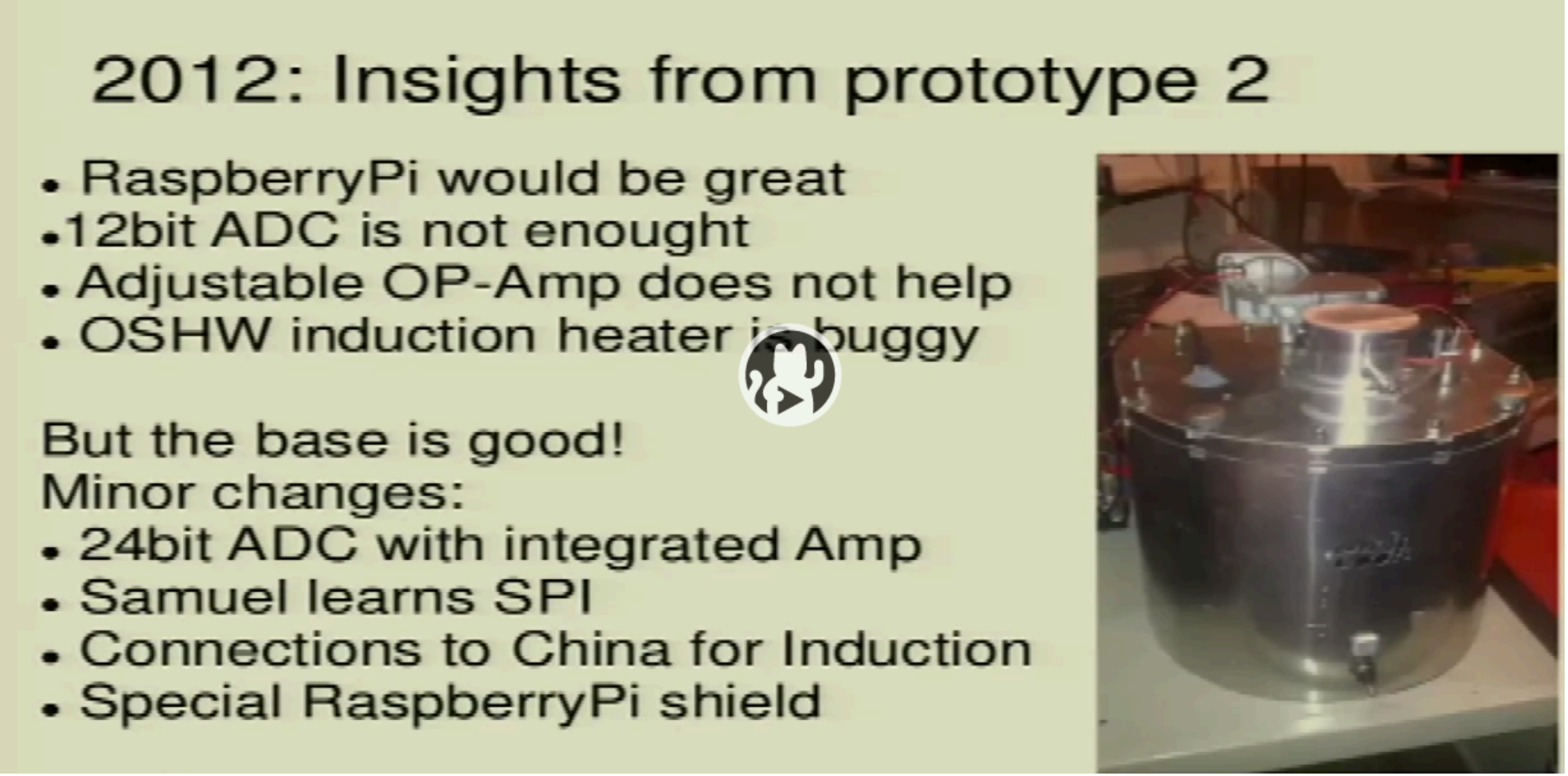
- Temperature or pressure
- Weight of added ingredient
- Rpm of stirring, runtime, pausetime
- Duration of step
- Stepmode



2011

- Make it real: First prototype
- Pressure cooker + fiberglass + epoxy
- Arduino + EEEpc
- Hacked induction heater
- Motor from trash
- Some lasercut parts
- Database as xml files
- Some php code
- Works!

Looks dangerous to Investors



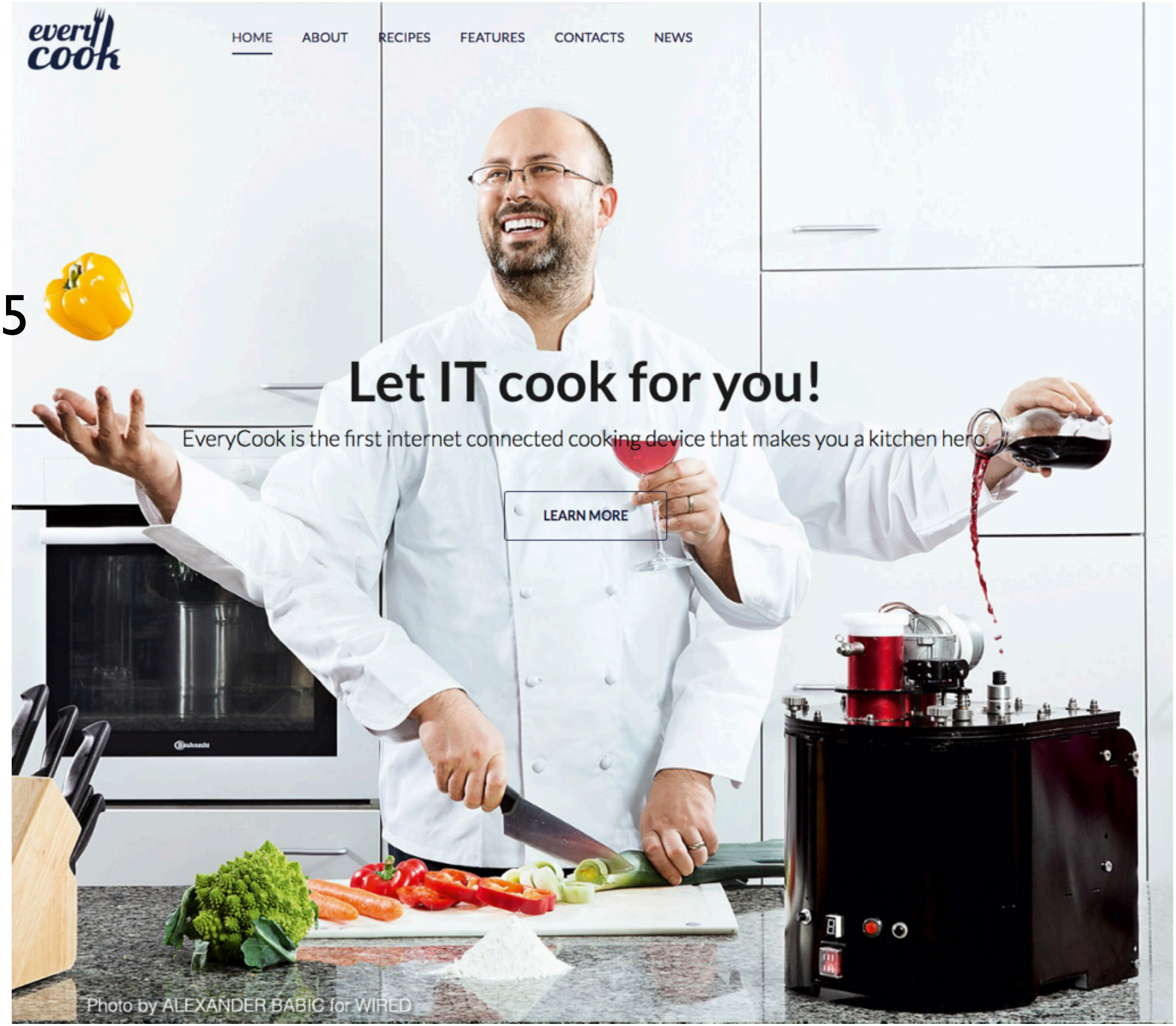
2012: Insights from prototype 2

- RaspberryPi would be great
- 12bit ADC is not enought
- Adjustable OP-Amp does not help
- OSHW induction heater is buggy

But the base is good!
Minor changes:

- 24bit ADC with integrated Amp
- Samuel learns SPI
- Connections to China for Induction
- Special RaspberryPi shield

2015



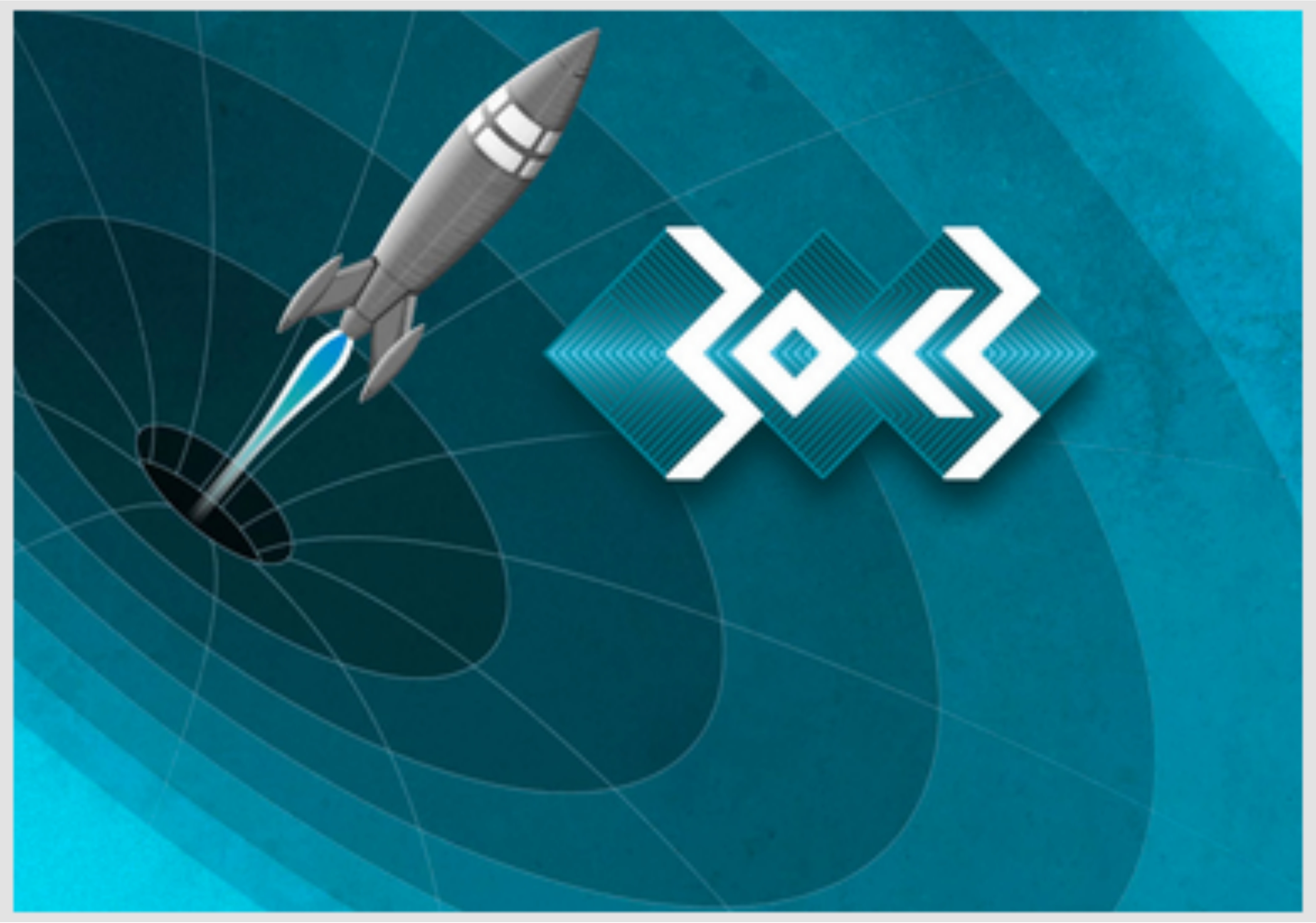
Let IT cook for you!

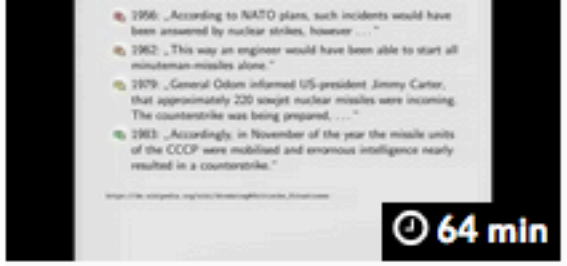
EveryCook is the first internet connected cooking device that makes you a kitchen hero.

Photo by ALEXANDER BABIC for WIRED

2013

30C3





- 1956: „According to NATO plans, such incidents would have been answered by nuclear strikes, however … .“
- 1962: „This way an engineer would have been able to start all minuteman-missiles alone.“
- 1979: „General Odom informed US-president Jimmy Carter, that approximately 220 sowjet nuclear missiles were incoming. The counterstrike was being prepared. … .“
- 1983: „Accordingly, in November of the year the missile units of the CCCP were mobilised and enormous intelligence nearly resulted in a counterstrike.“

64 min

We only have one earth

A case for expansionistic space policy

2013-12-28 72 Drahflow

- Digital Fabrication – everthing is a file and fits into a directory structure.
- All parts are ready to enter an additive or subtractive manufacturing process.
- Tasks can easily be assigned to individual team member

33 min

Structuring open hardware projects

experiences from the "i3 Berlin" 3D printer project with...

2013-12-29 67 Bram de Vries and Morris Winkler

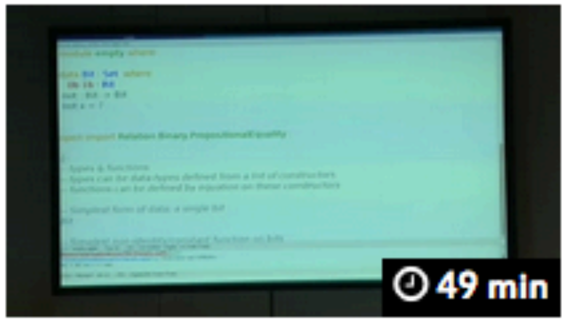
„Identity Media are available in many formats, such as smart cards, security chips embedded in personal computers, cell phones, software based certificates, and Universal Serial Bus (USB) devices. Selecting the appropriate identity medium and credential type is implementation-specific and depends on the risk tolerance of the participating entities. “

(NSTIC Page 22)

63 min

Europe, the USA and Identity Ecosystems

2013-12-29 63 NoisyNarrowBandDevice



49 min

BREACH in Agda

Security notions, proofs and attacks using dependently...

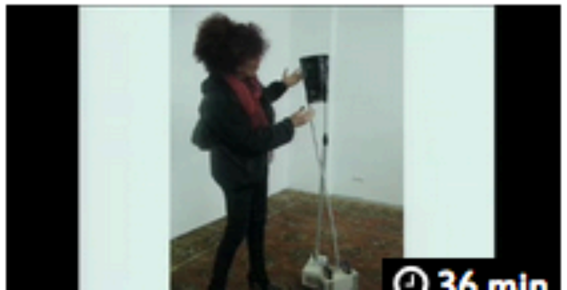
2013-12-28 57 Nicolas Pouillard

33 min

Open source experimental incubator build up

call for participation in project and product development

2013-12-28 50 Frantisek Algoldor Apfelbeck



36 min

Sim Gishel

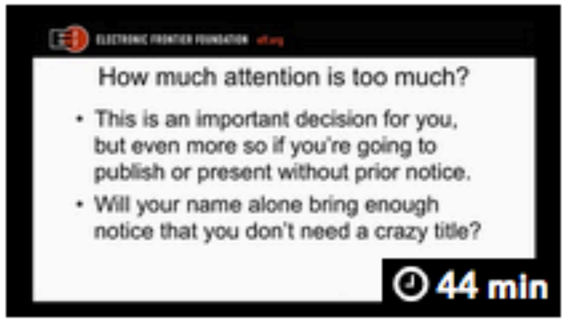
A singing and dancing robot build to take part in casting...

2013-12-27 40 Karl Heinz Jeron

IFGINT

Erkenntnisse aus Informationsfreiheitsanfragen - Hacks,...

2013-12-27 88 Stefan Wehrmeyer



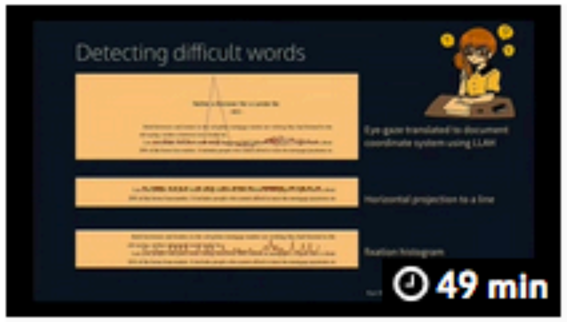
How much attention is too much?

- This is an important decision for you, but even more so if you're going to publish or present without prior notice.
- Will your name alone bring enough notice that you don't need a crazy title?

Disclosure DOs, Disclosure DON'Ts

Pragmatic Advice for Security Researchers

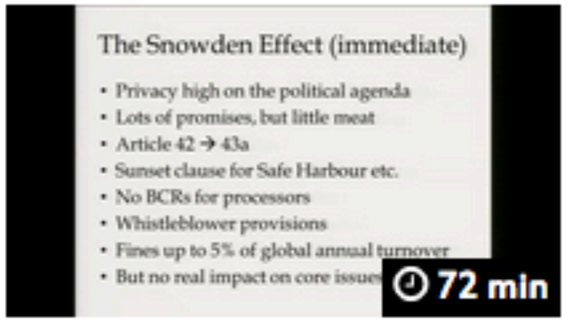
2013-12-28 85 Nate Cardozo


Detecting difficult words
Eye gaze translated to document coordinate system using LLAH
Horizontal projection to a line
fixation histogram
49 min

Toward a Cognitive "Quantified Self"

Activity Recognition for the Mind

2013-12-27 83 Kai

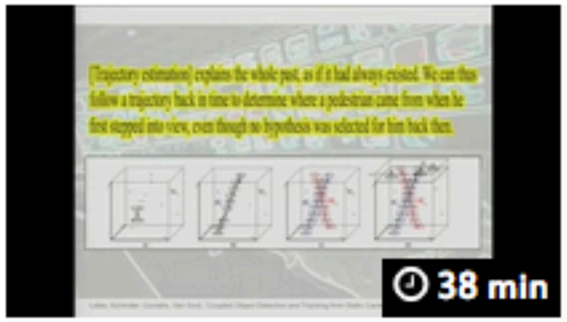


The Snowden Effect (immediate)

- Privacy high on the political agenda
- Lots of promises, but little meat
- Article 42 → 43a
- Sunset clause for Safe Harbour etc.
- No BCRs for processors
- Whistleblower provisions
- Fines up to 5% of global annual turnover
- But no real impact on core issues

EUDataP: State of the Union

2013-12-28 78 Jan Philipp Albrecht

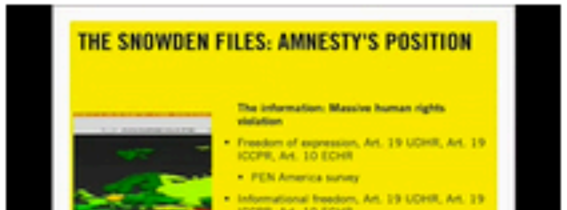


[Trajectory estimation] explains the whole past, as if it had always existed. We can thus follow a trajectory back in time to determine where a pedestrian came from when he first stepped into view, even though no hypothesis was selected for him back then.

Policing the Romantic Crowd

Velocipedes and Face Recognition

2013-12-27 76 MaTu



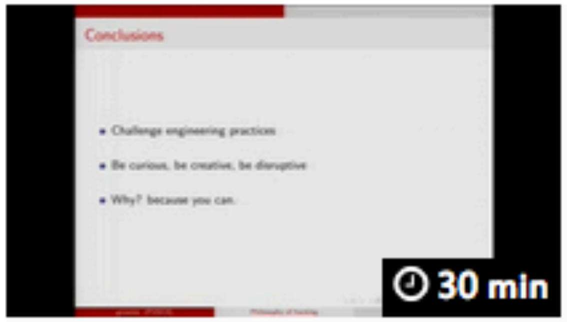
THE SNOWDEN FILES: AMNESTY'S POSITION

The information: Massive human rights violation

- Freedom of expression, Art. 19 UDHR, Art. 19 ICCPR, Art. 10 ECHR
  - PEN America survey
- Informational freedom, Art. 19 UDHR, Art. 19

Human Rights and Technology

"A New Hope" or "The Empire Strikes Back"?



Conclusions

- Challenge engineering practices
- Be curious, be creative, be disruptive
- Why? because you can.

The philosophy of hacking

Contemplations on the essence of hacking and its...

📅 2013-12-30 👁 126 👤 groente

Network effect

The more people use a given communication platform, the more people will start using it

Technomonopolies

How technology is used to subvert and circumvent...

📅 2013-12-28 👁 122 👤 rysiek

Problem: private keys security/safety

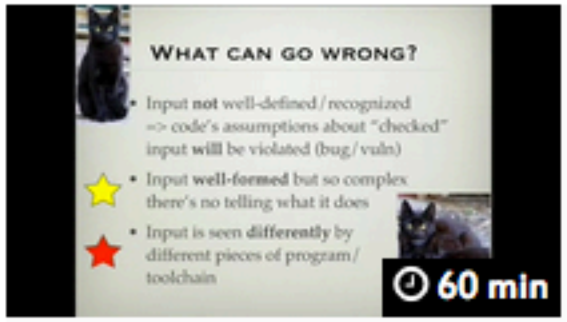
- end user computer security
  - compromised computers
  - untrusted computers
  - rigged clients
- data (wallet) loss
  - disasters, hard-drive failures
  - naive reinstalls
  - failing to do proper backups

Trezor: Bitcoin hardware wallet

📅 2013-12-29 👁 119 👤 Pavol "stick" Rusnak

Towards an affordable brain-computer-interface

📅 2013-12-29 👁 117 👥 Dominic and Anne

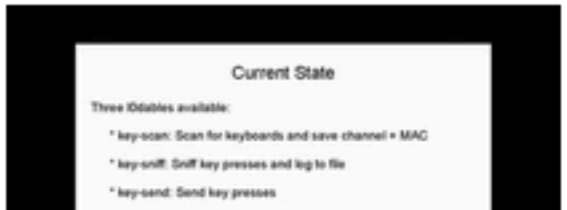


WHAT CAN GO WRONG?

- Input **not** well-defined / recognized => code's assumptions about "checked" input **will** be violated (bug / vuln)
- Input **well-formed** but so complex there's no telling what it does
- Input is seen **differently** by different pieces of program / toolchain

Revisiting "Trusting Trust" for binary toolchains

📅 2013-12-28 👁 114 👥 sergeybratus, Julian Bangert and bx



Current State

Three IOdables available:

* key-scan: Scan for keyboards and save channel + MAC
* key-sniff: Sniff key presses and log to file
* key-send: Send key presses

Lightning Talks, Day 3

Hacking as Artistic Practice

!Mediengruppe Bitnik about their recent works

📅 2013-12-28 👁 155 👥 !Mediengruppe Bitnik and !Mediengruppe Bitnik

Turing Complete User

What can be done to protect the term, the notion and the...

📅 2013-12-28 👁 155 👤 olia lialina

Rock' em Graphic Cards

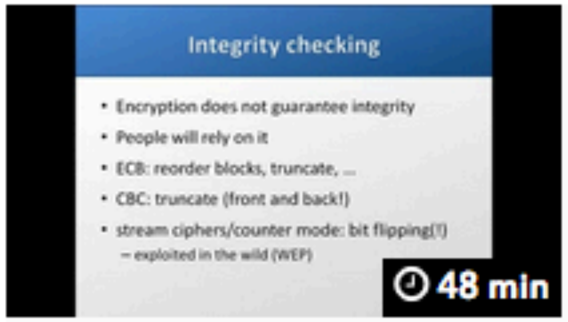
Introduction to Heterogeneous Parallel Programming

📅 2013-12-27 👁 151 👤 mel/ Agnes Meyder

Foundation of the European Pirate Party (PPEU)
Manifesto of the European Pirate Party
Civil Rights
Citizen participation and Open Government
Transparency
Copyright reform
Patent system reform
Open Access and Open Data
Net Neutrality
Free software and Libre Culture
153 min

Lightning Talks, Day 4

📅 2013-12-30 👁 143 👤 nickfarr


Integrity checking
Encryption does not guarantee integrity
People will rely on it
ECB: reorder blocks, truncate, ...
CBC: truncate (front and back!)
stream ciphers/counter mode: bit flipping(!)
– exploited in the wild (WEP)
48 min

Reverse engineering of CHIASMUS from GSTOOL

It hurts.

📅 2013-12-27 👁 141 👤 Jan Schejbal

Desperately Seeking Susy

A farewell to a bold proposal?

Forbidden Fruit

2013-12-27 196 Joe Davis

#SOPA, #NSA, and the New Internet "Lobby"

2013-12-29 195 Elizabeth Stark

lasers in space

more than just pew pew!

2013-12-27 184 anja

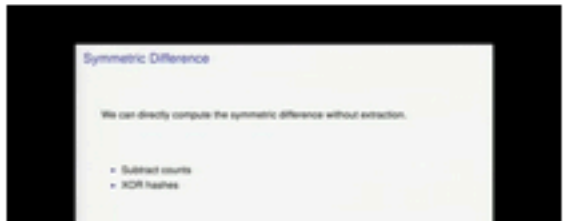
Glass Hacks

Fun and frightening uses of always-on camera enabled...

2013-12-28 173 Stephen Balaban

Lightning Talks, Day 2

2013-12-28 169 nickfarr


Symmetric Difference
We can directly compute the symmetric difference without extraction.
Subtract counts
XOR hashes

The GNU Name System

A Decentralized PKI For Social Movements

Method Parameter Manipulation : the details

- The DVM needs to know how big the method arguments are
  - insSize
  - We also set registersSize == insSize
- Argument size calculation
  - Every argument adds one (1) to the input size
  - J (a double) adds two (2)
  - For methods of object classes (non static classes) add one (1) for the instance (this)

```
java.lang.String.compareTo("Ljava/lang/String;)I
insSize == 2
```

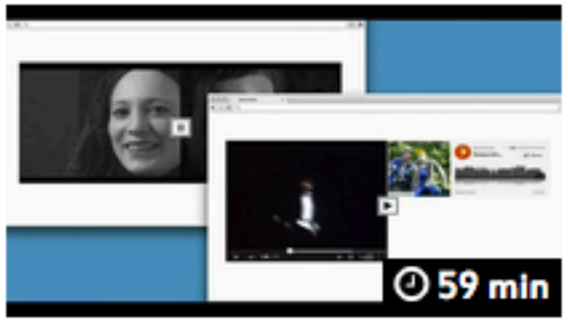
Collin Mulliner – "Android DDI: Dynamic Dalvik Instrumentation" –

47 min

Android DDI

Dynamic Dalvik Instrumentation of Android Applications and...

2013-12-29 209 Collin Mulliner



59 min

Recht auf Remix

2013-12-29 206 Leonhard Dobusch

PSHDL

Plain and Simple HDL

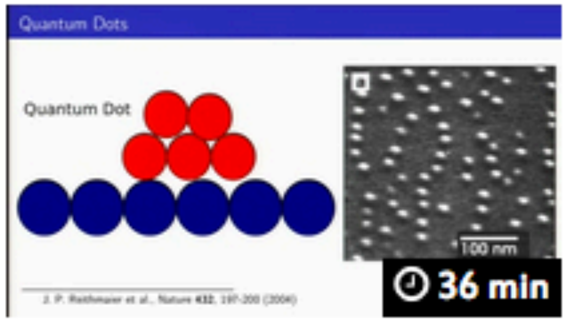
Creating the Arduino for FPGAs

61 min

Programming FPGAs with PSHDL

Let's create the Arduino for FPGAs

2013-12-28 205 Karsten Becker



Quantum Dots

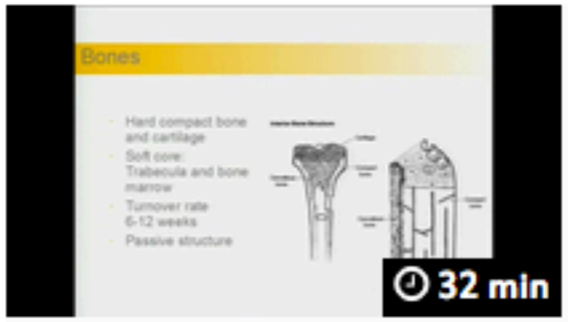
J. P. Reithmaier et al., Nature 432, 197-200 (2004)

36 min

Long Distance Quantum Communication

Concepts and components for intercontinal communication...

2013-12-27 204 C B



Bones

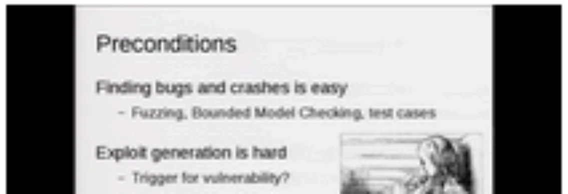
- Hard compact bone and cartilage
- Soft core: Trabecula and bone marrow
- Turnover rate 6-12 weeks
- Passive structure

32 min

Coding your body

How to decipher the messages of your body

2013-12-30 204 Sophie Hiltner



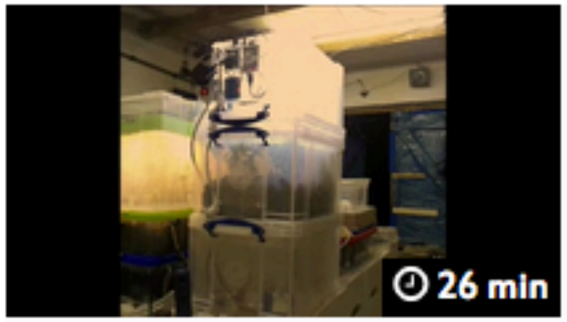
Preconditions

Finding bugs and crashes is easy
- Fuzzing, Bounded Model Checking, test cases

Exploit generation is hard
- Trigger for vulnerability?

Triggering Deep Vulnerabilities Using Symbolic Execution

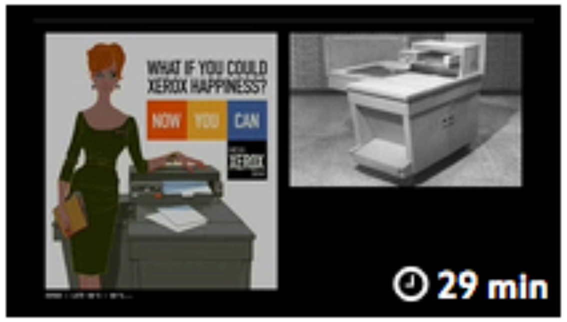
Deep program analysis without the headache



Plants & Machines

Food replicating Robots from Open Source Technologies

2013-12-28 267 mrv and bbuegler



The Pirate Cinema

Creating mash-up movies by hidden activity and geography of...

2013-12-28 261 Nicolas Maigret and Brendan Howell

Data Execution Prevention
• Enforces code integrity on page granularity
– Execute code if eXecutable bit set
• W^X ensures write access or executable
– Mitigates against code corruption attacks
– Low overhead, hardware enforced, widely deployed
• Weaknesses and limitations
– No-self modifying code supported
56 min

WarGames in memory

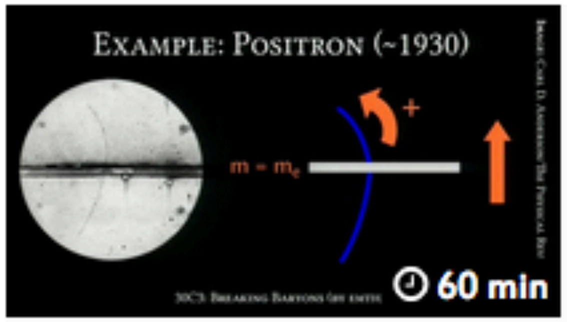
what is the winning move?

2013-12-29 259 gannimo

Data Mining for Good

Using random sampling, entity resolution, communications...

2013-12-29 254 Patrick



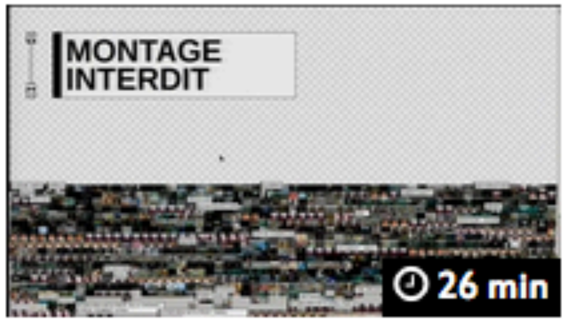
Breaking Baryons

On the Awesomeness of Particle Accelerators and Colliders

2013-12-27 252 Michael Büker

The Four Wars

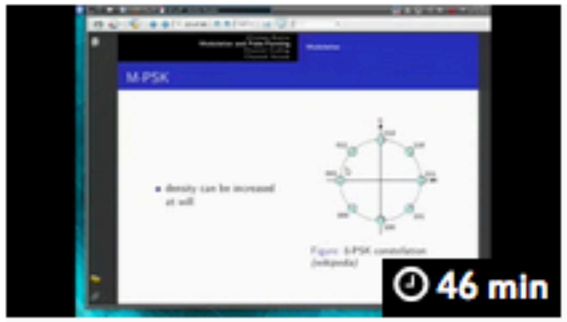
Terror, whistleblowers, drugs, internet



Against Metadata

Twisting time and space to explore the unknown

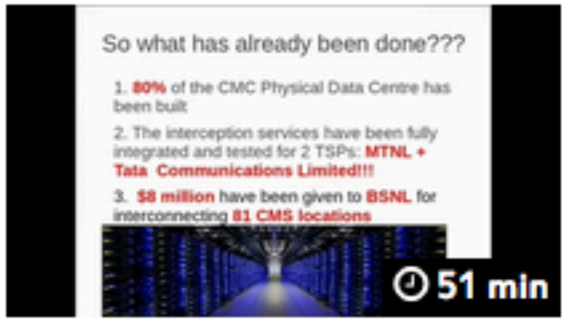
📅 2013-12-28 👁 354 👤 Robert M Ochshorn



Basics of Digital Wireless Communication

introduction to software radio principles

📅 2013-12-27 👁 343 👤 Clemens Hopfer


So what has already been done???

1. 80% of the CMC Physical Data Centre has been built
2. The interception services have been fully integrated and tested for 2 TSPs: MTNL + Tata Communications Limited!!!
3. $8 million have been given to BSNL for interconnecting 81 CMS locations

India's Surveillance State

📅 2013-12-29 👁 337 👤 Maria Xynou

HbbTV Security

OMG - my Smart TV got pr0wn3d

📅 2013-12-27 👁 330 👤 Martin Herfurt

Other Interesting Vectors

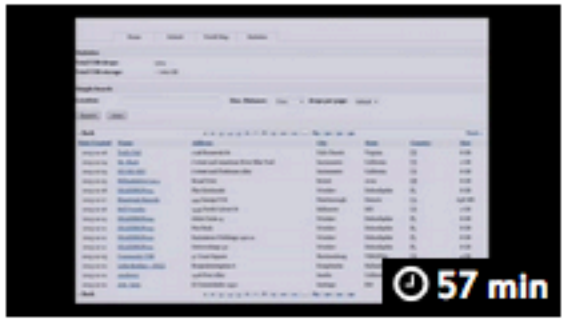
- Intentional misconfiguration
  - It is possible to misconfigure PCIe config space, MSRs or MMIO constants in order to create unexpected situations for the VMM
- Server platforms (are fun!)
  - Platforms and CPUs for the server market have special features, all of those usually run in very high privilege
- Errata
  - What if there is an Errata in the CPU/PCH
    rely on to emulate something - sucks, ri

Virtually Impossible: The Reality Of Virtualization Security

Errata FTW

📅 2013-12-29 👁 313 👤 Gal Diskin

Amtliche Datenschützer: Kontrolleure oder Papiertiger?

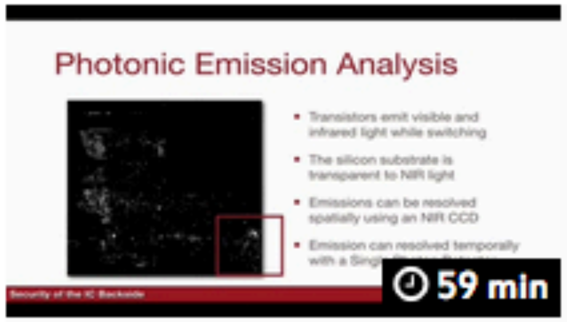


57 min

Hello World!

How to make art after Snowden?

2013-12-28 · 419 · Aram Bartholl



Photonic Emission Analysis

- Transistors emit visible and infrared light while switching
- The silicon substrate is transparent to NIR light
- Emissions can be resolved spatially using an NIR CCD
- Emission can resolved temporally with a Sing

Security of the IC Backside

59 min

Security of the IC Backside

The future of IC analysis

2013-12-28 · 418 · nedos

ELECTRONIC FRONTIER FOUNDATION eff.org

What are your responsibilities?

1. To get it right

2. To communicate your advice in way that is understood by your audience

62 min

The Internet (Doesn't) Need Another Security Guide

Creating Internet Privacy and Security Resources That Don't...

2013-12-29 · 408 · evacide

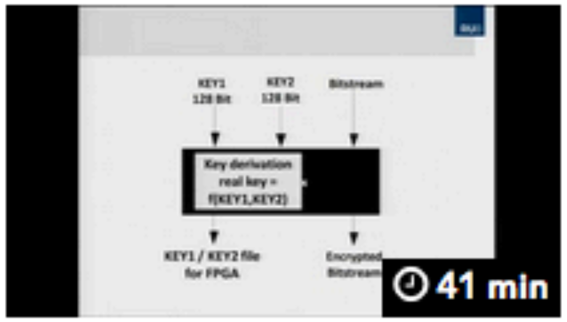
Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

44 min

Backdoors, Government Hacking and The Next Crypto Wars

2013-12-29 · 385 · Christopher Soghoian



41 min

Extracting keys from FPGAs, OTP Tokens and Door Locks

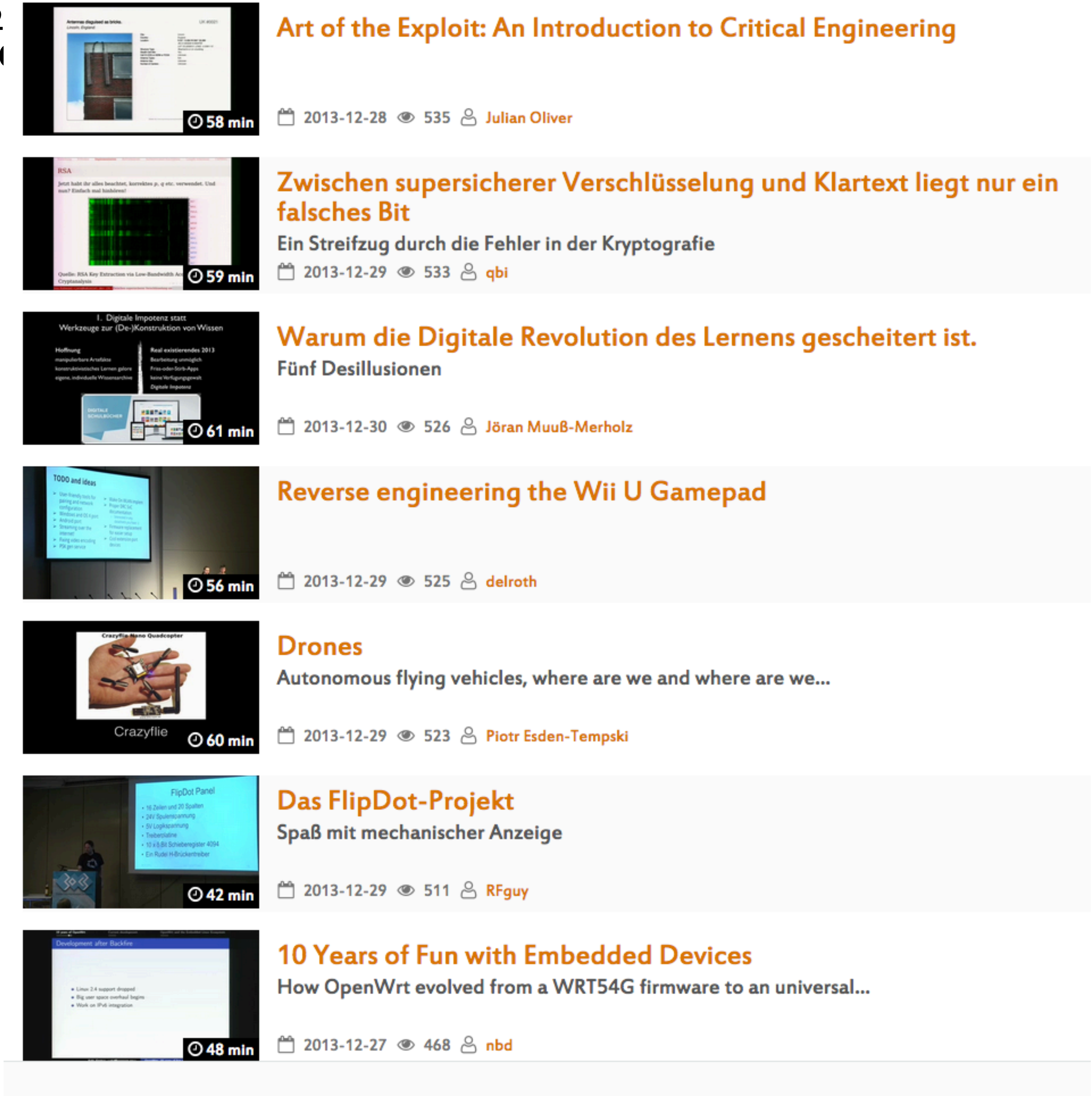
Side-Channel (and other) Attacks in Practice

2013-12-28 · 384 · David

Do You Think That's Funny?

Art Practice under the Regime of Anti-Terror Legislation

2
3(



Art of the Exploit: An Introduction to Critical Engineering

58 min

2013-12-28 535 Julian Oliver

Zwischen supersicherer Verschlüsselung und Klartext liegt nur ein falsches Bit

Ein Streifzug durch die Fehler in der Kryptografie

59 min

2013-12-29 533 qbi

Warum die Digitale Revolution des Lernens gescheitert ist.

Fünf Desillusionen

61 min

2013-12-30 526 Jöran Muuß-Merholz

Reverse engineering the Wii U Gamepad

56 min

2013-12-29 525 delroth

Drones

Autonomous flying vehicles, where are we and where are we...

60 min

2013-12-29 523 Piotr Esden-Tempski

Das FlipDot-Projekt

Spaß mit mechanischer Anzeige

42 min

2013-12-29 511 RFguy

10 Years of Fun with Embedded Devices

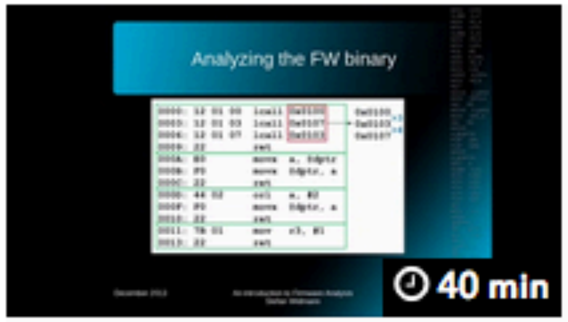
How OpenWrt evolved from a WRT54G firmware to an universal...

48 min

2013-12-27 468 nbd

Anonymity and Privacy in Public Space and on the Internet

2013-12-29 439 aluburka



An introduction to Firmware Analysis

Techniques - Tools - Tricks

2013-12-27 437 Stefan Widmann

SCADA StrangeLove 2

We already know

2013-12-28 436 repdet and sgordey

Meet SoftBoundCETS
Santosh Nagarakatte, Jianzhou Zhao, Milo M. K. Martin, Steve Zdancewic; UPenn
SoftBound: spatial safety
CETS: temporal safety
Uses disjoint fat pointers
Proof of correctness (but caveat emptor)
Implemented as LLVM optimizer pass
47 min

Bug class genocide

Applying science to eliminate 100% of buffer overflows

2013-12-27 436 Andreas Bogk

FPGA 101

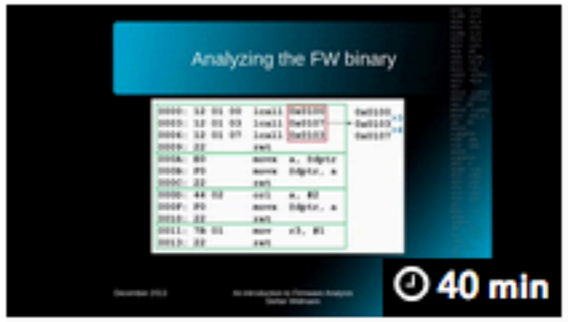
Making awesome stuff with FPGAs

2013-12-28 432 Karsten Becker

The good, the bad, and the ugly - Linux Kernel patches

Anonymity and Privacy in Public Space and on the Internet

2013-12-29 439 aluburka



An introduction to Firmware Analysis

Techniques - Tools - Tricks

2013-12-27 437 Stefan Widmann

SCADA StrangeLove 2

We already know

2013-12-28 436 repdet and sgordey

Meet SoftBoundCETS
Santosh Nagarakatte, Jianzhou Zhao, Milo M. K. Martin, Steve Zdancewic; UPenn
SoftBound: spatial safety
CETS: temporal safety
Uses disjoint fat pointers
Proof of correctness (but caveat emptor)
Implemented as LLVM optimizer pass
47 min

Bug class genocide

Applying science to eliminate 100% of buffer overflows

2013-12-27 436 Andreas Bogk

FPGA 101

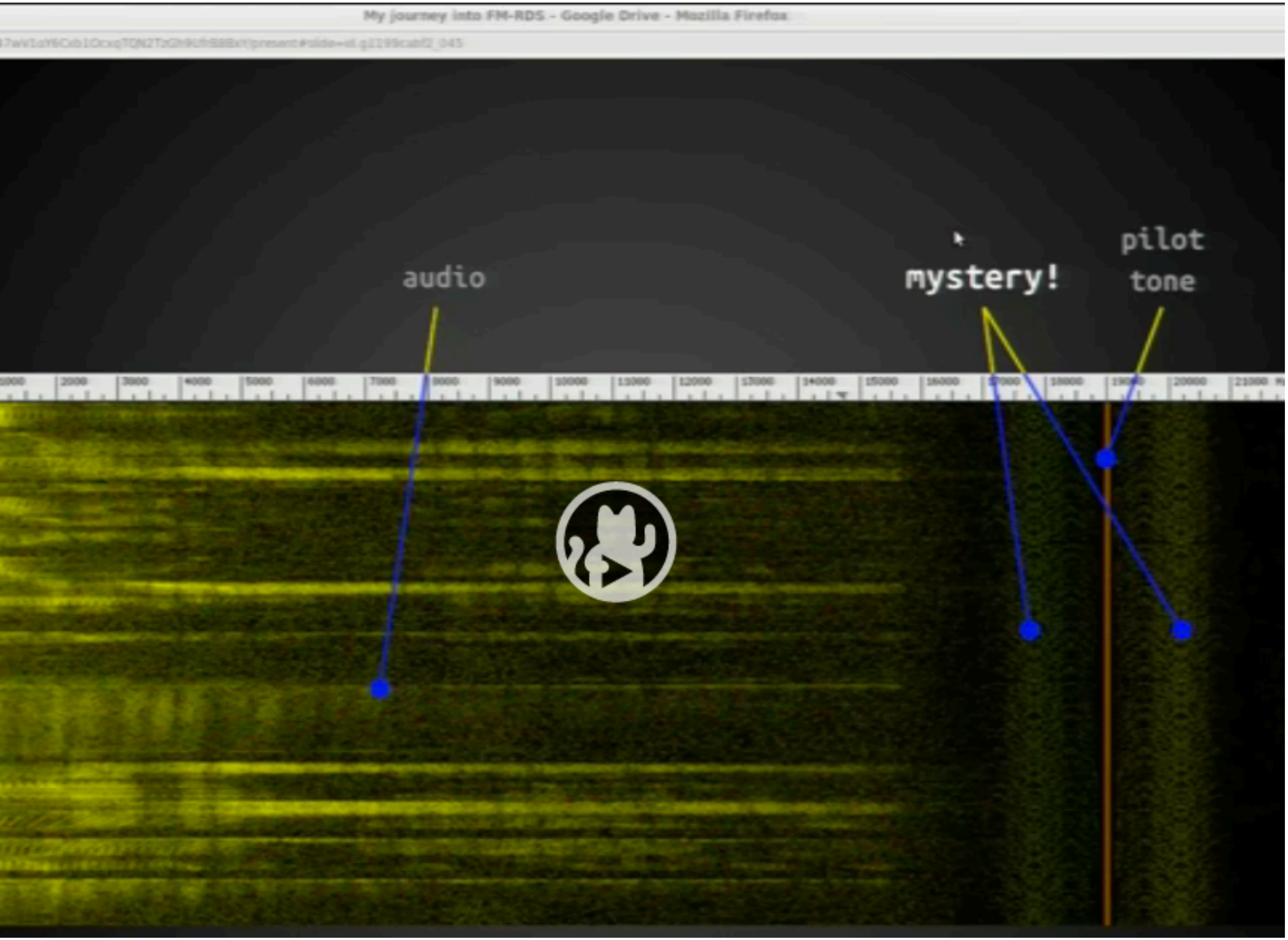
Making awesome stuff with FPGAs

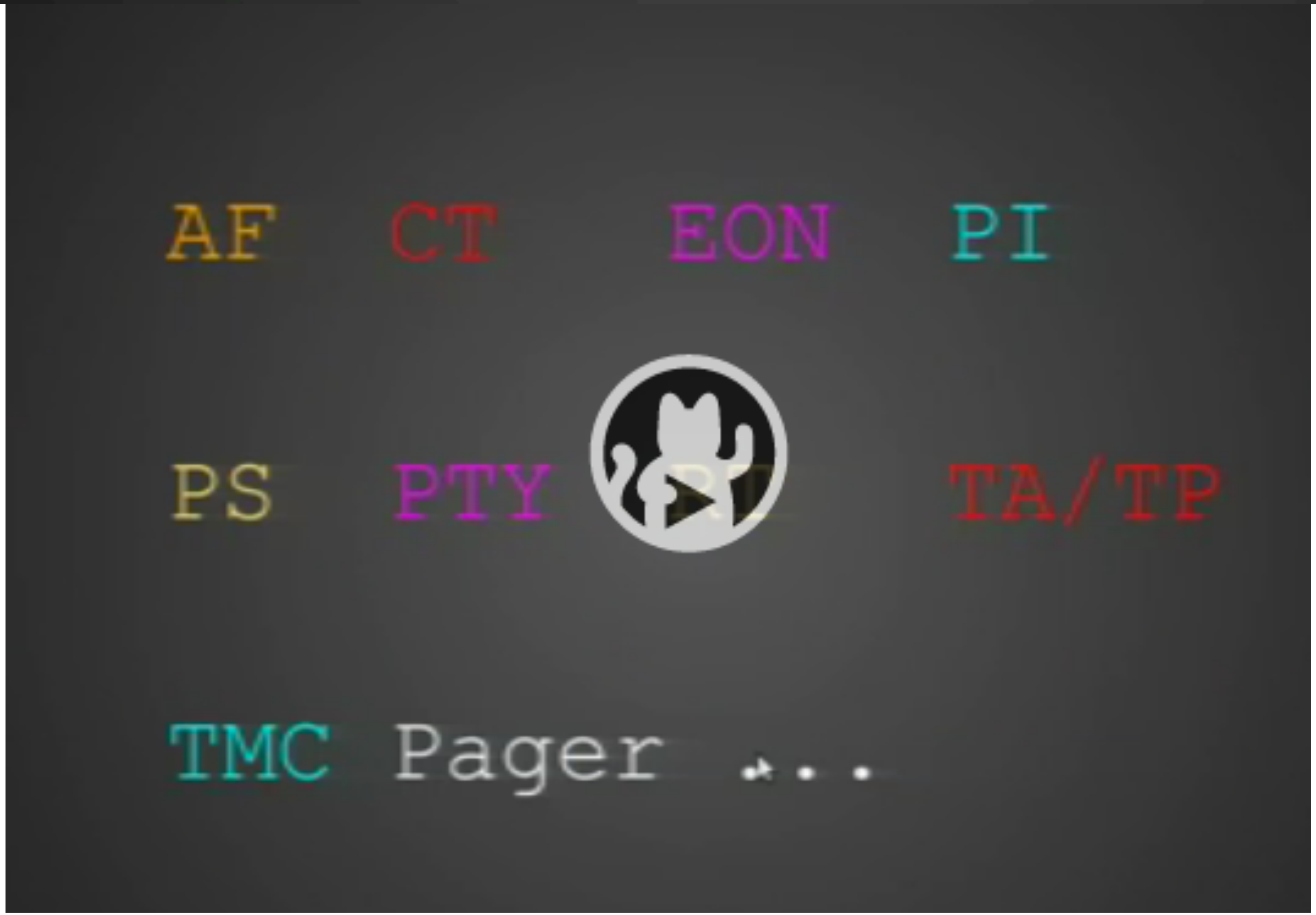
2013-12-28 432 Karsten Becker

The good, the bad, and the ugly - Linux Kernel patches

ourney into FM-RDS

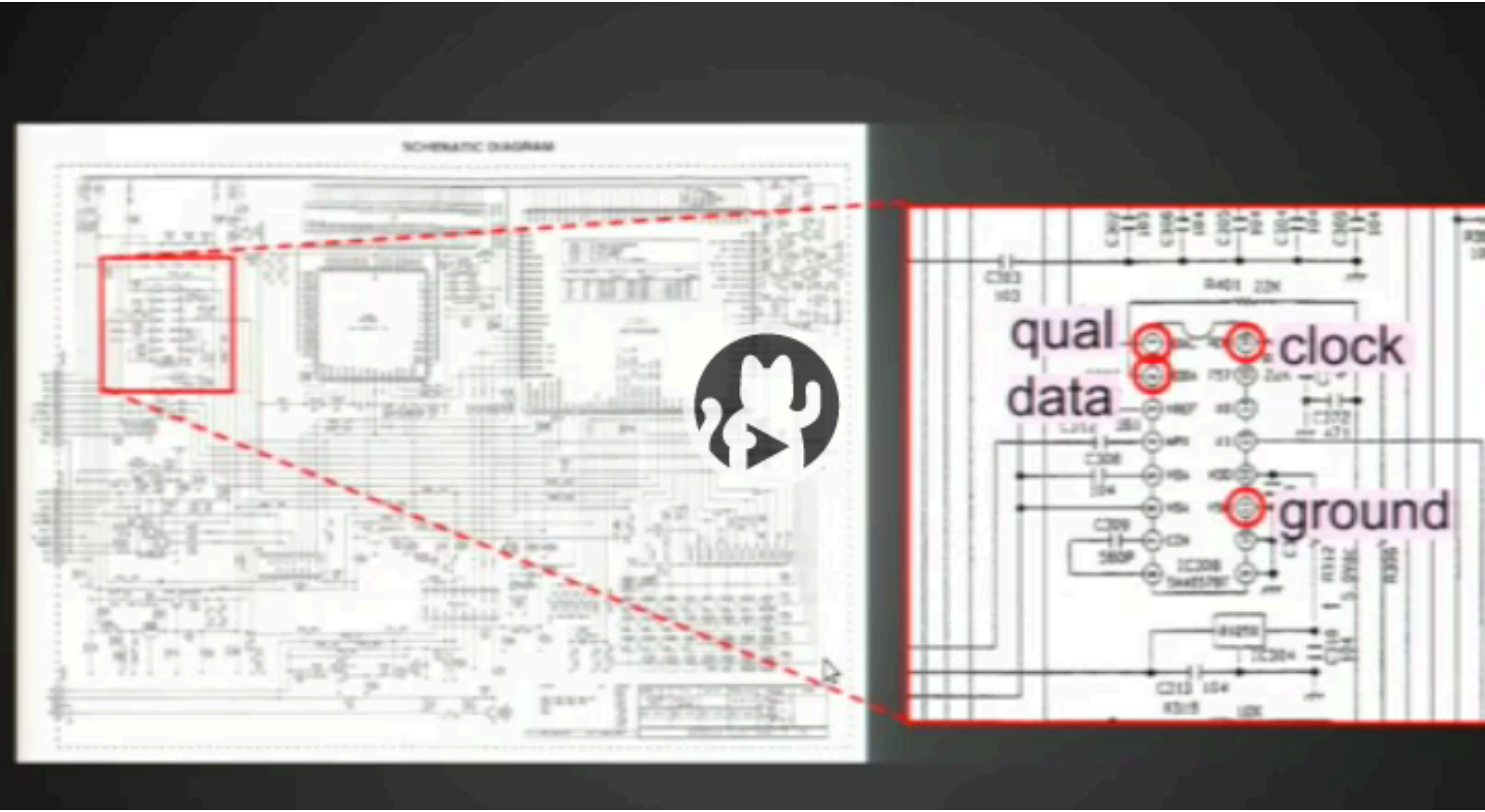
nen

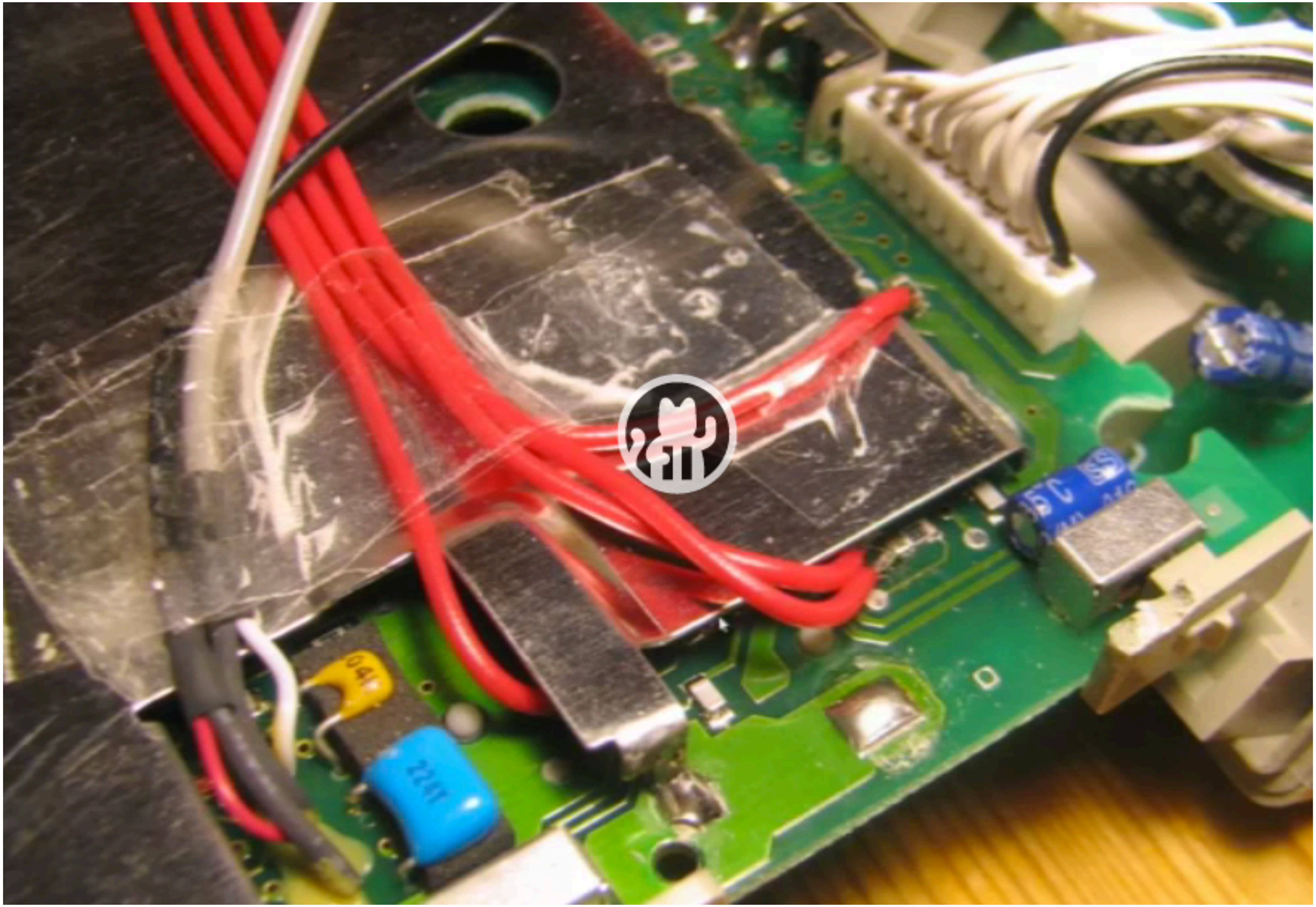


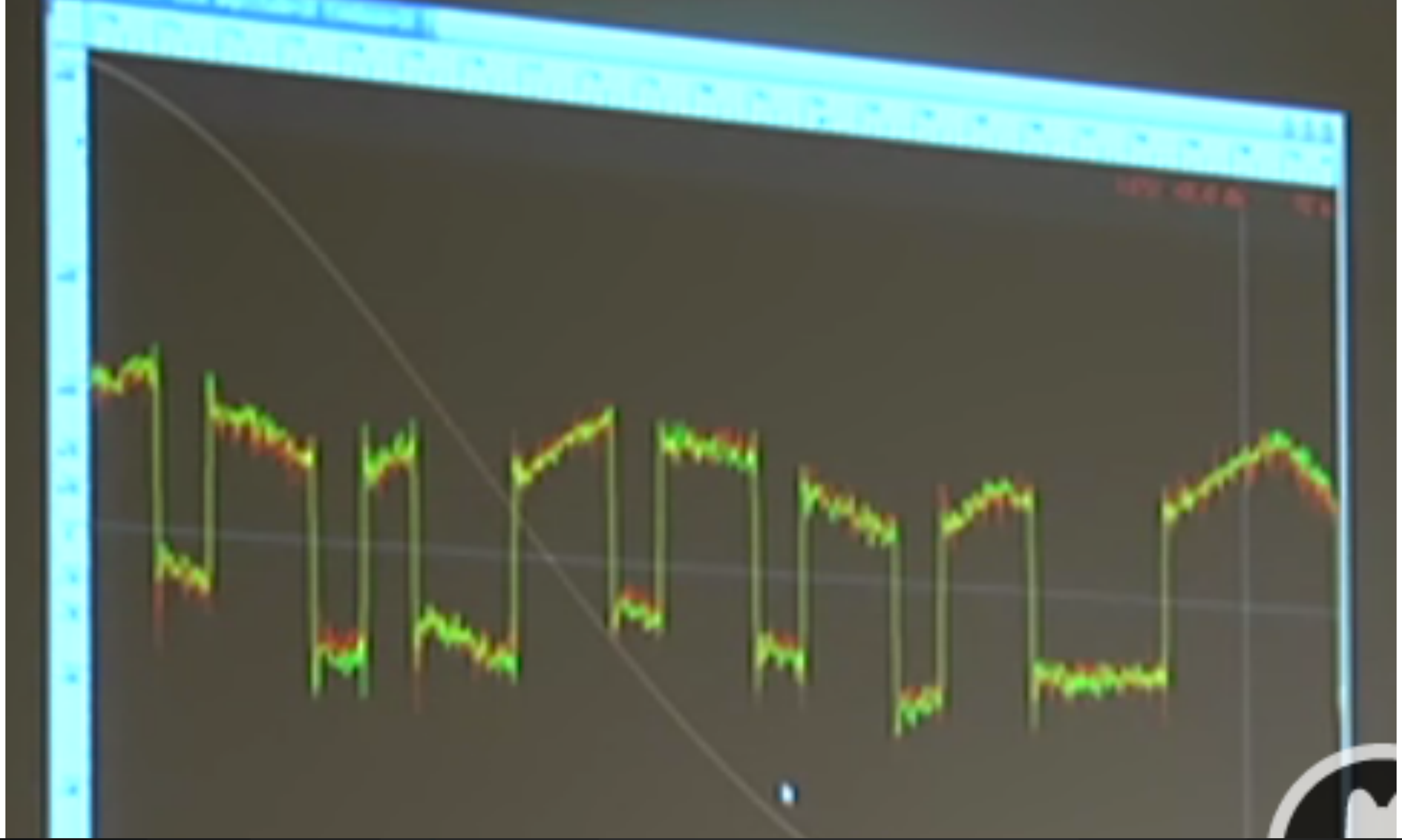

AF CT EON PI

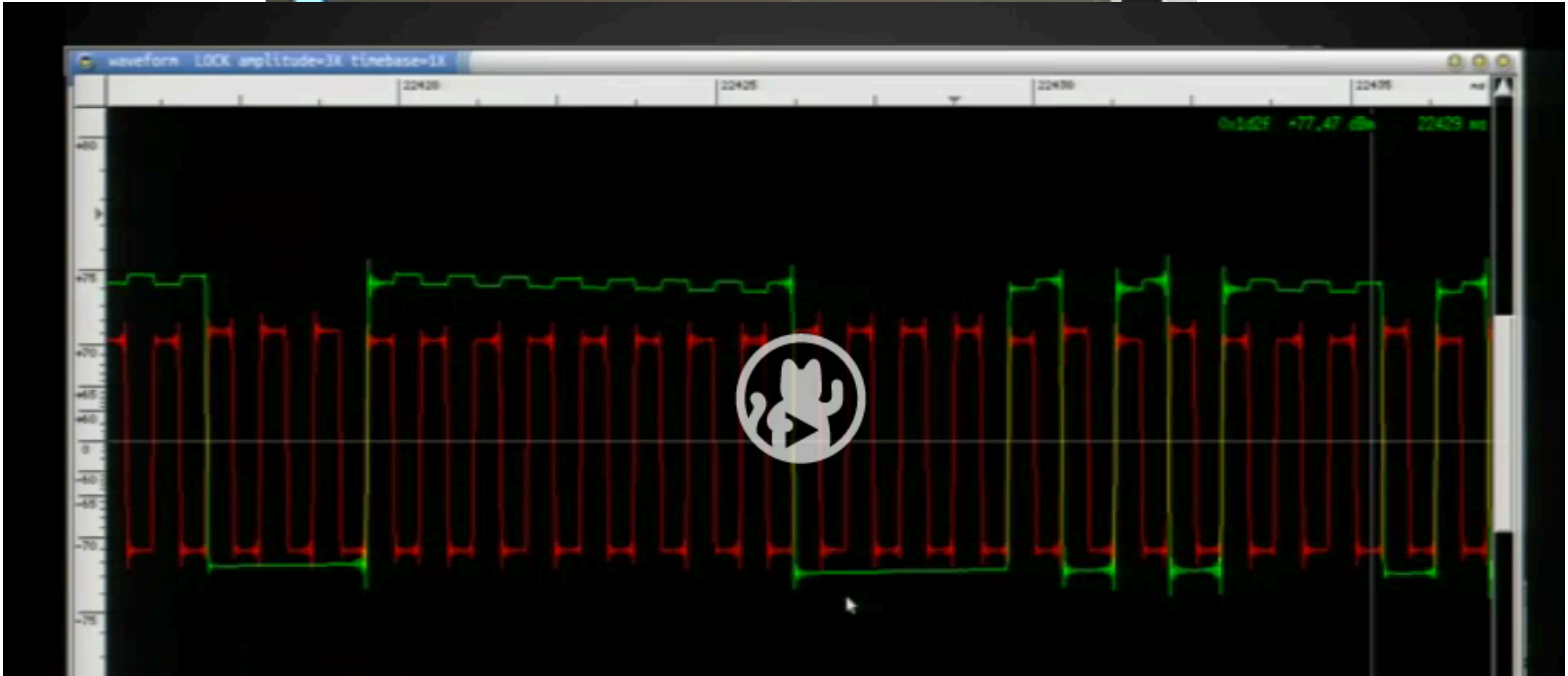
PS PTY RT TA/TP

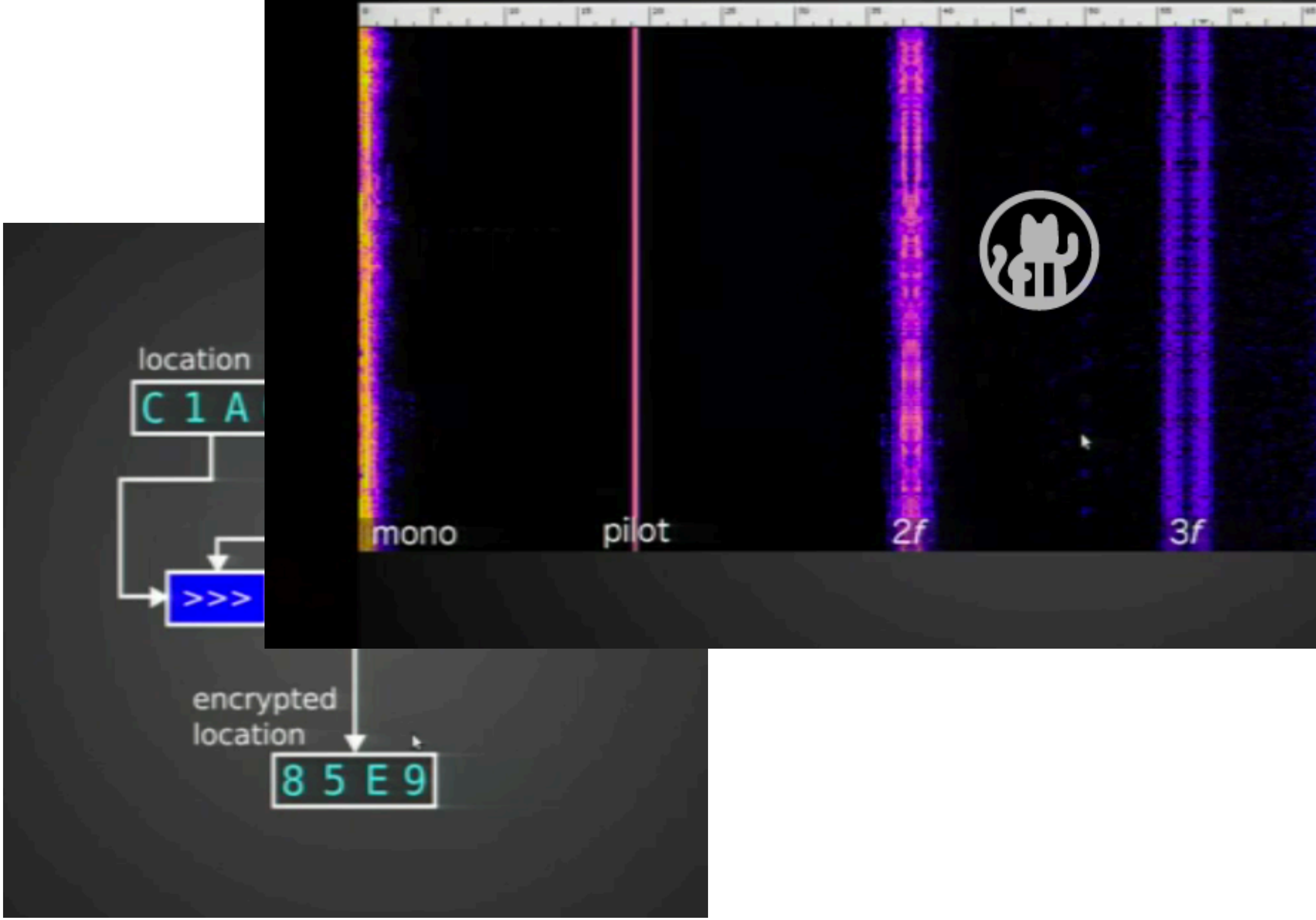
TMC Pager ...

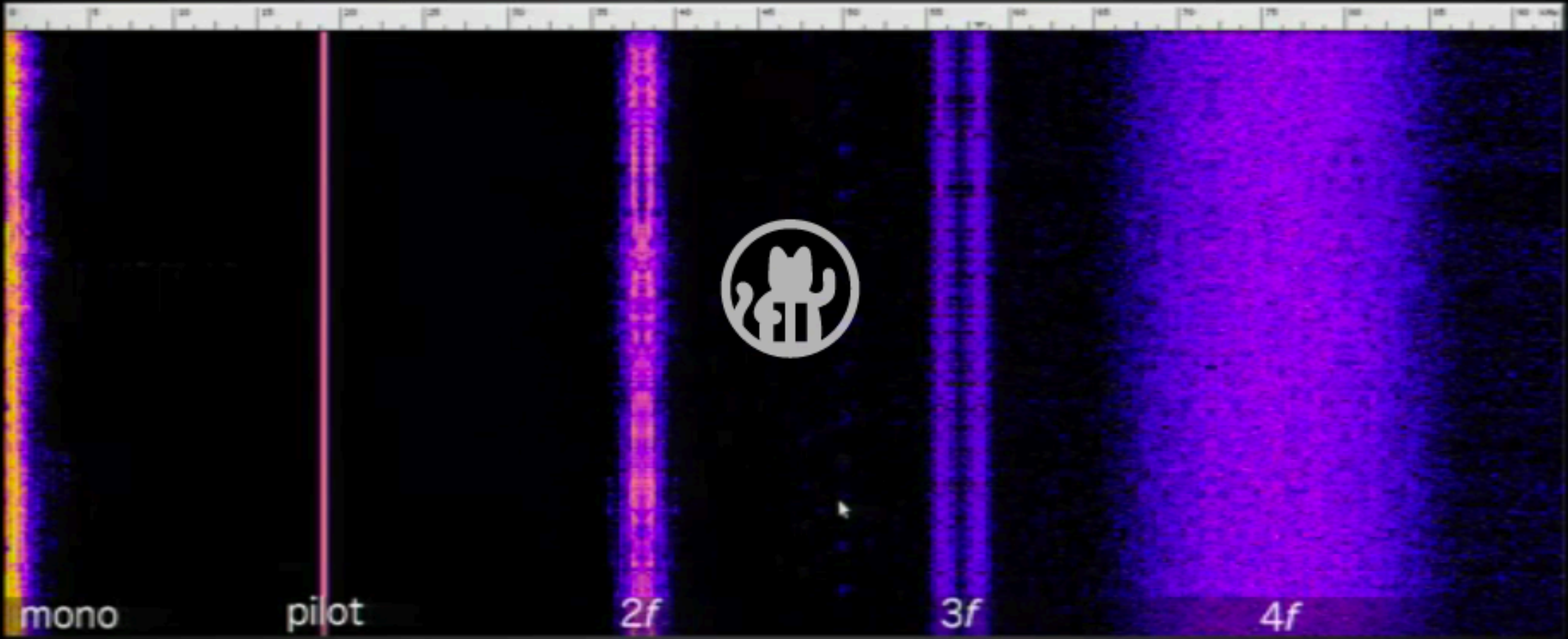

SCHEMATIC DIAGRAM
C303
103
R401 22K
qual
data
clock
C308
104
C309
560P
IC208
ground
IC204
C212 104
R315
10K

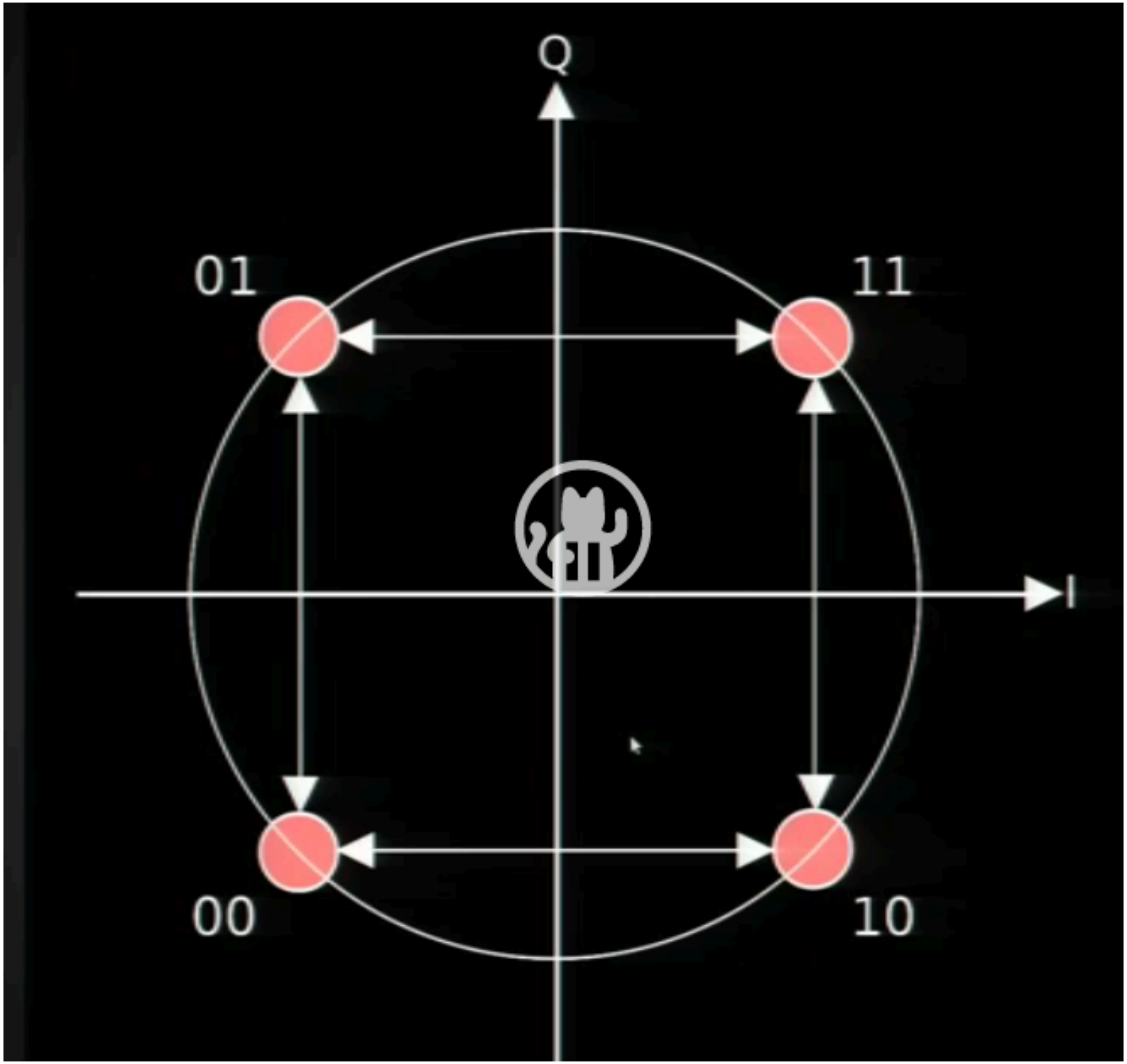


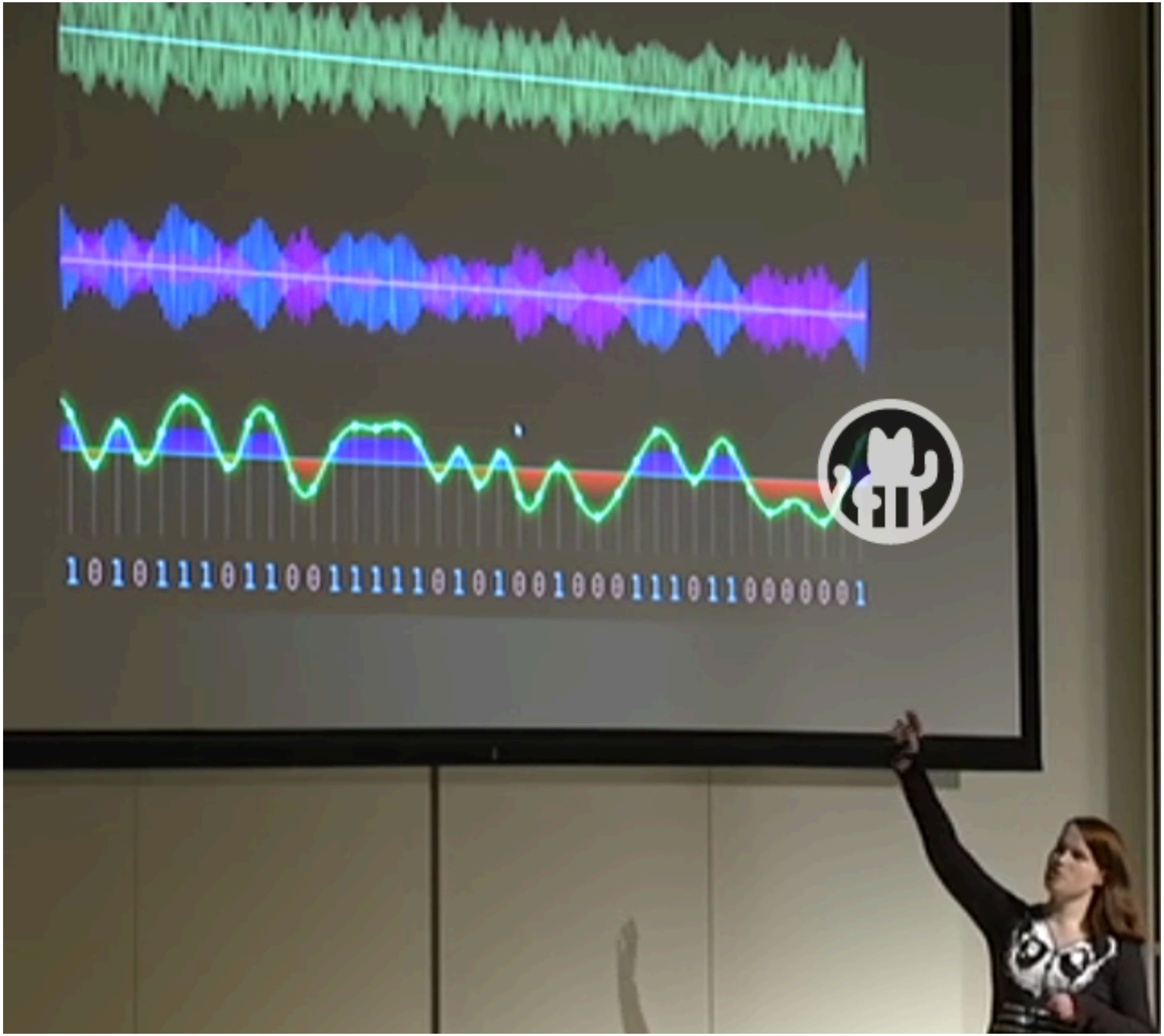



waveform LOCK amplitude=3X timebase=1X
22420
22425
22430
22435
ms
0x1d29 +77.47 dBm 22429 ms

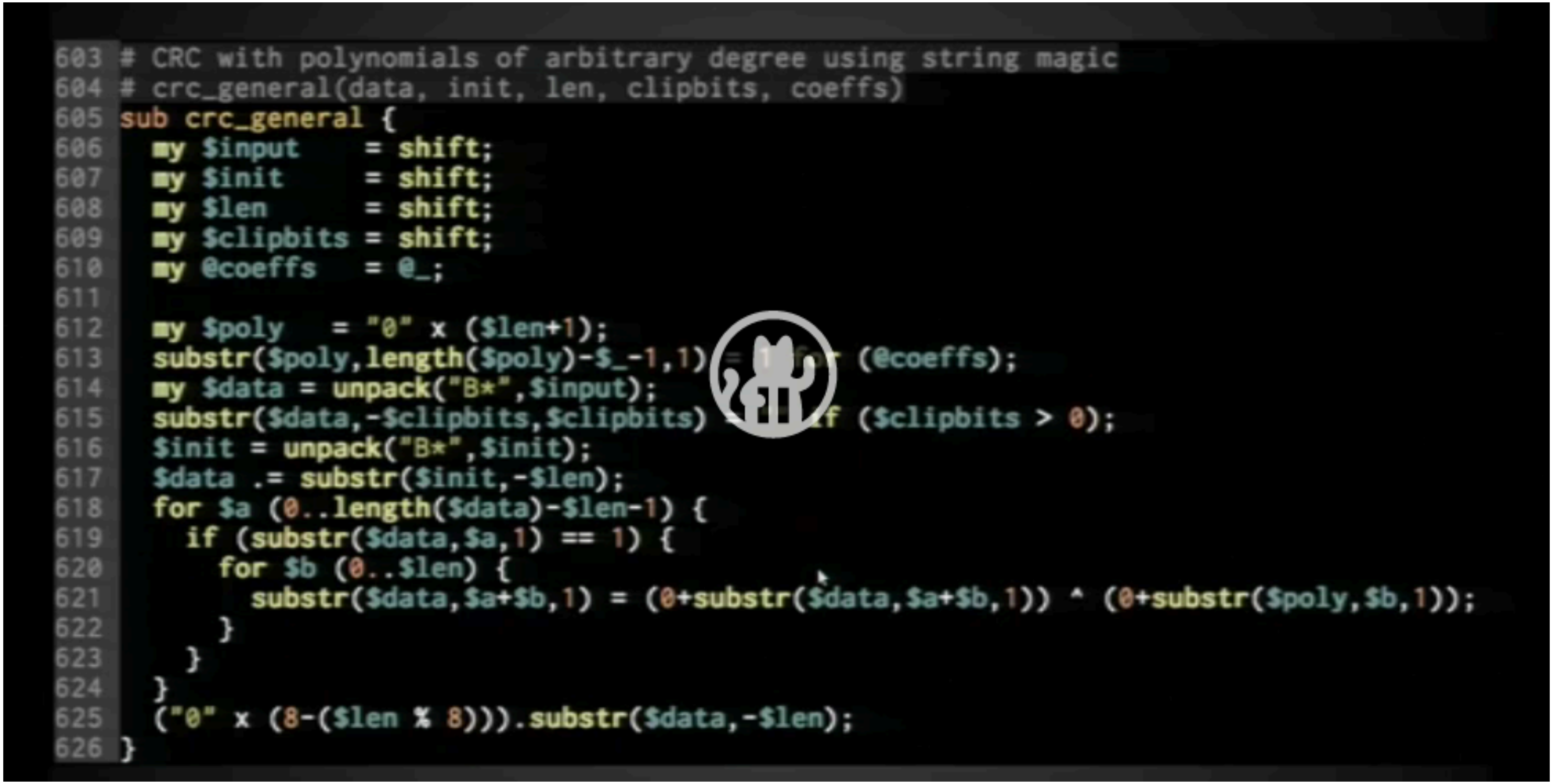

location
C 1 A
>>>
encrypted location
8 5 E 9
mono
pilot
2f
3f


mono
pilot
2f
3f
4f

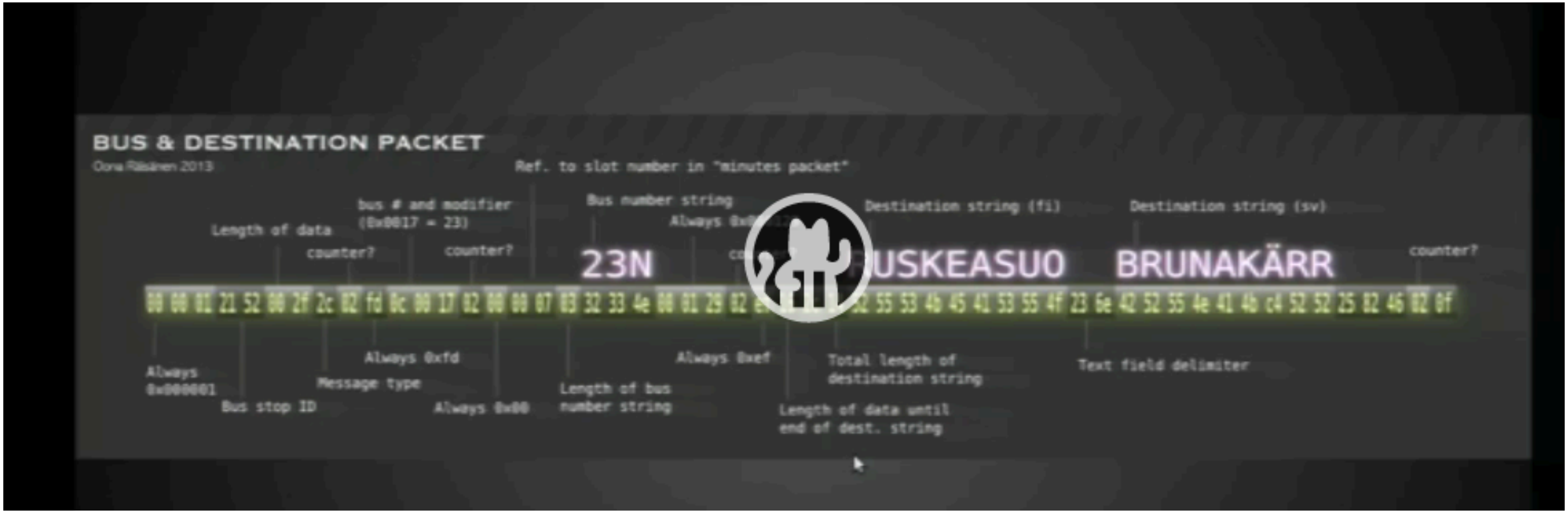

Q
I
01
11
00
10



1010111011001111101010010001110110000001



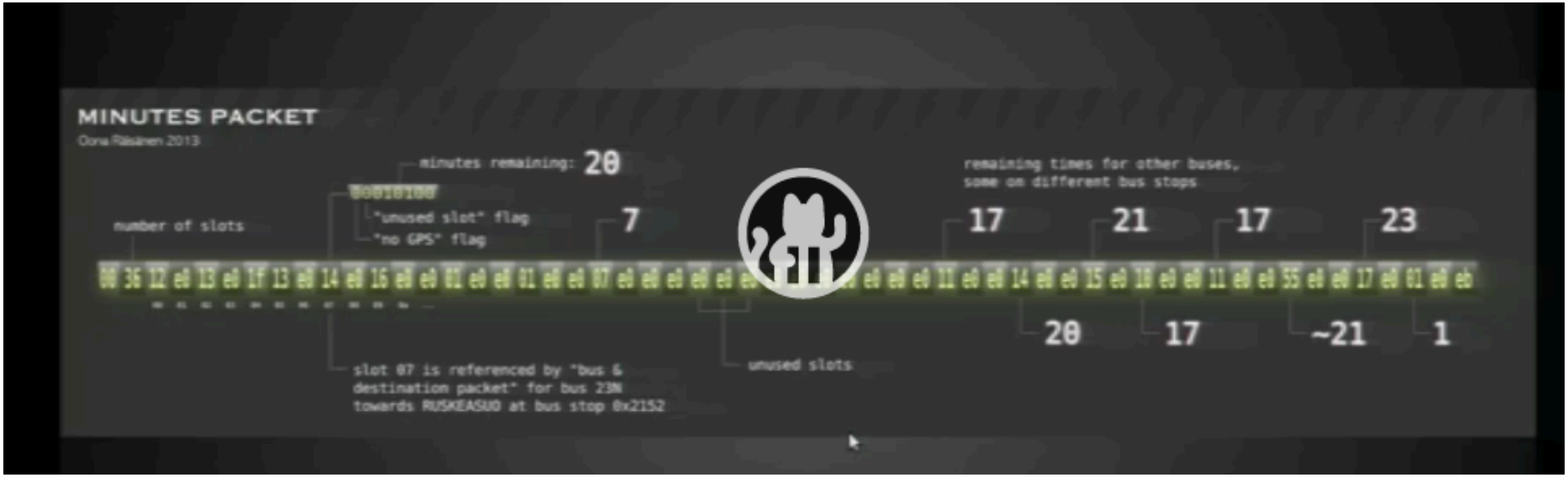
```perl
# CRC with polynomials of arbitrary degree using string magic
# crc_general(data, init, len, clipbits, coeffs)
sub crc_general {
  my $input    = shift;
  my $init     = shift;
  my $len      = shift;
  my $clipbits = shift;
  my @coeffs   = @_;

  my $poly   = "0" x ($len+1);
  substr($poly,length($poly)-$_-1,1) = 1 for (@coeffs);
  my $data = unpack("B*",$input);
  substr($data,-$clipbits,$clipbits) = "" if ($clipbits > 0);
  $init = unpack("B*",$init);
  $data .= substr($init,-$len);
  for $a (0..length($data)-$len-1) {
    if (substr($data,$a,1) == 1) {
      for $b (0..$len) {
        substr($data,$a+$b,1) = (0+substr($data,$a+$b,1)) ^ (0+substr($poly,$b,1));
      }
    }
  }
  ("0" x (8-($len % 8))).substr($data,-$len);
}
```



BUS & DESTINATION PACKET

Oona Räisänen 2013

```
00 00 01 21 52 00 2f 2c 02 fd 0c 00 17 02 00 00 07 03 32 33 4e 00 01 29 02 e[illegible] [illegible] 52 55 53 4b 45 41 53 55 4f 23 6e 42 52 55 4e 41 4b c4 52 52 25 02 46 02 0f
```

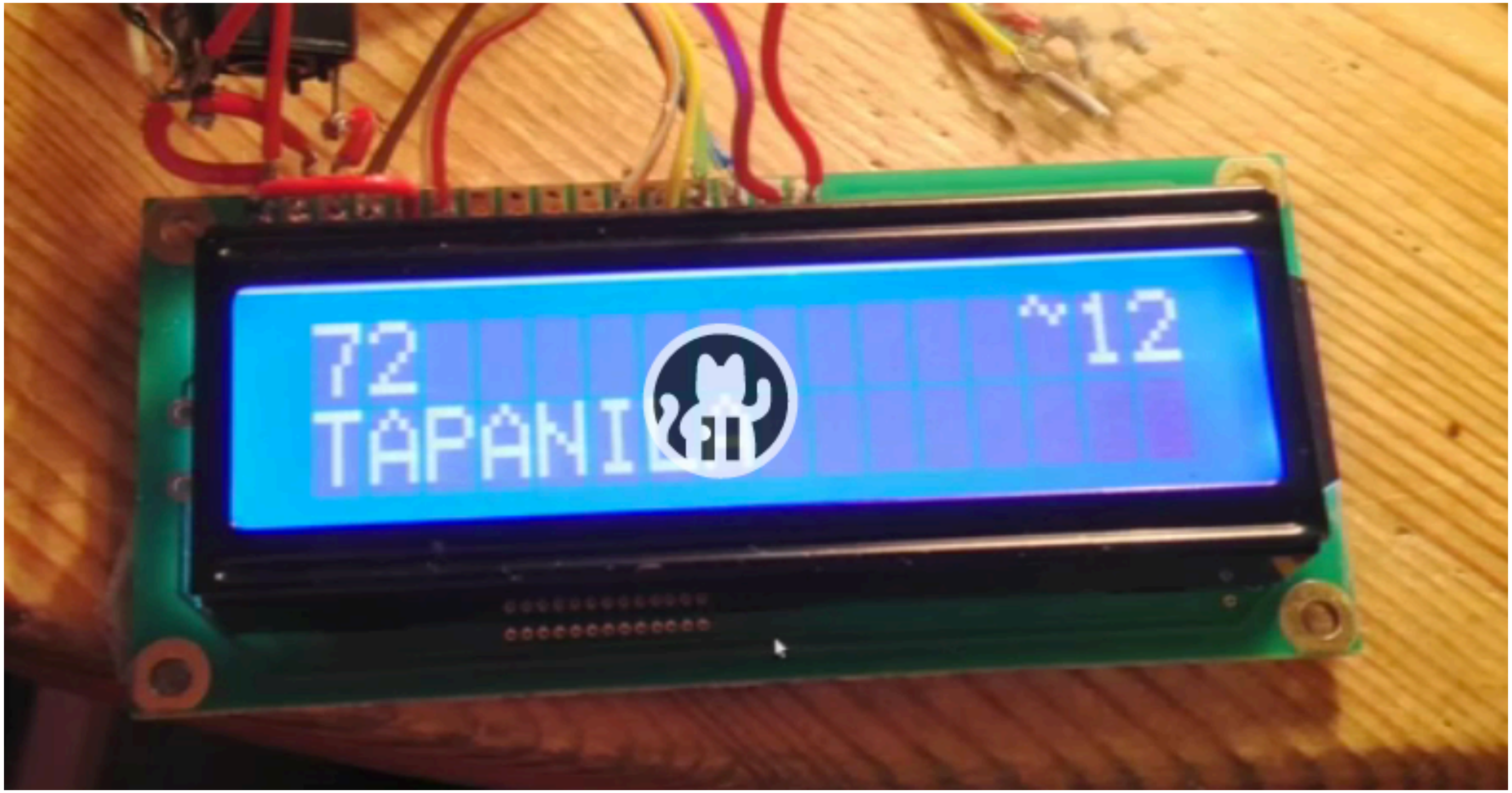


MINUTES PACKET

Oona Räisänen 2013

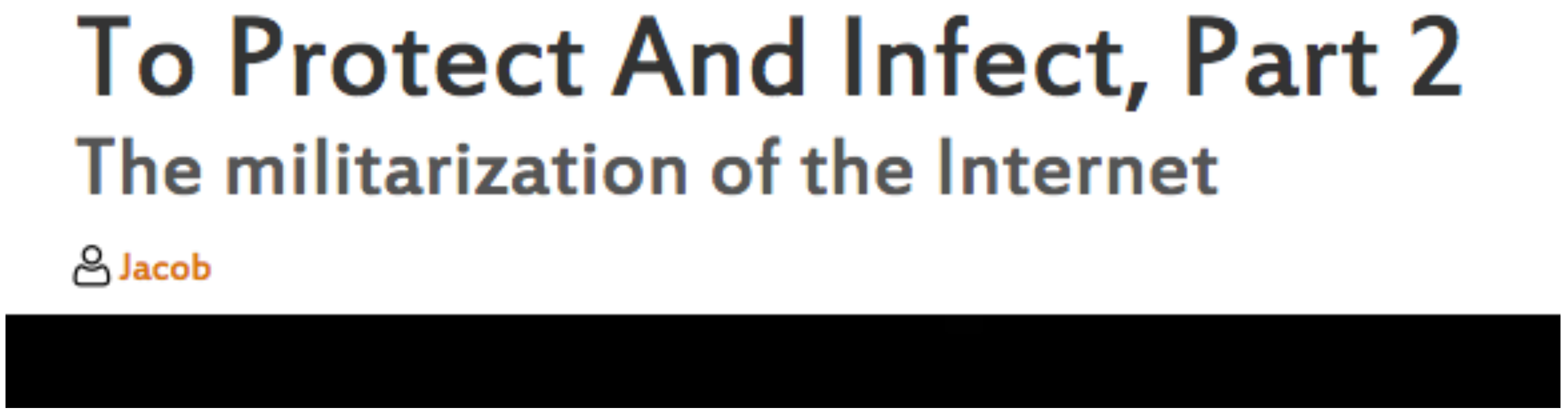
```
00 36 12 e0 13 e0 1f 13 e0 14 e0 16 e0 e0 01 e0 e0 01 e0 e0 07 e0 e0 e0 e0 e0 e0 [illegible] e0 e0 e0 11 e0 e0 14 e0 e0 15 e0 10 e0 e0 11 e0 e0 55 e0 e0 17 e0 01 e0 eb
```

slot 07 is referenced by "bus & destination packet" for bus 23N towards RUSKEASUO at bus stop 0x2152



http://www.windytan.com/

2013
30C3



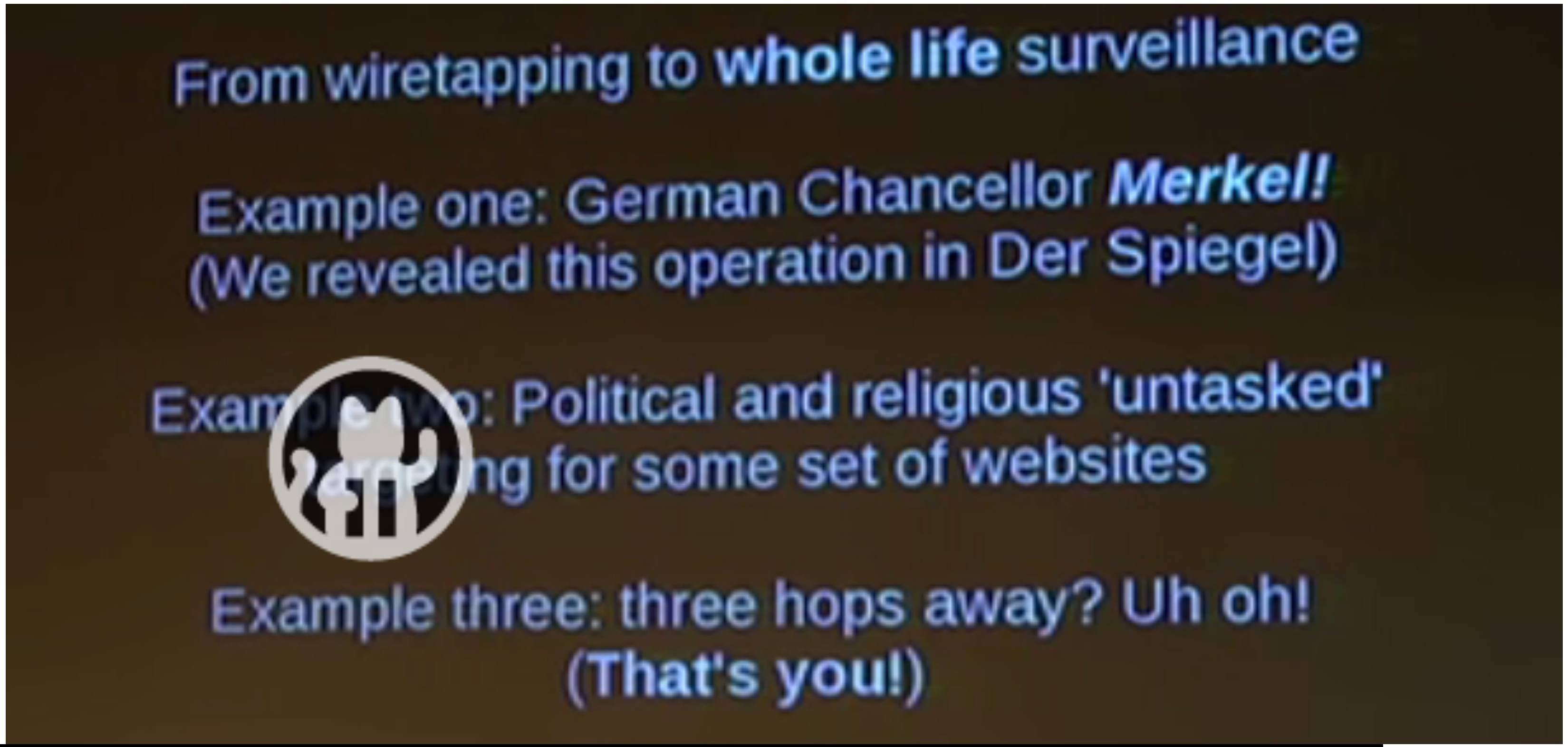
To Protect And Infect, Part 2

The militarization of the Internet

Jacob

[redacted]

2013
30C3

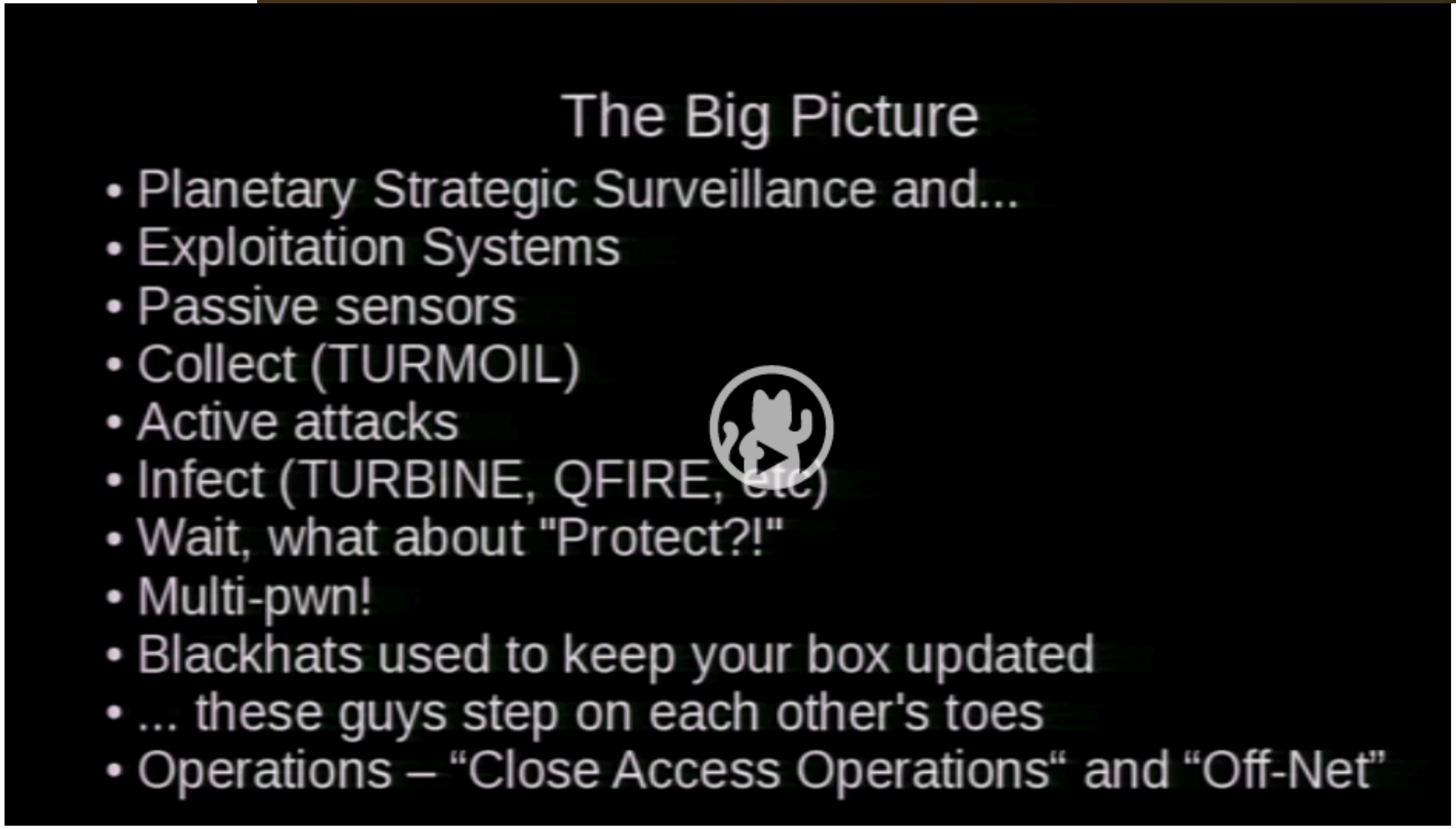


From wiretapping to **whole life** surveillance

Example one: German Chancellor ***Merkel!***
(We revealed this operation in Der Spiegel)

Example two: Political and religious 'untasked'
targeting for some set of websites

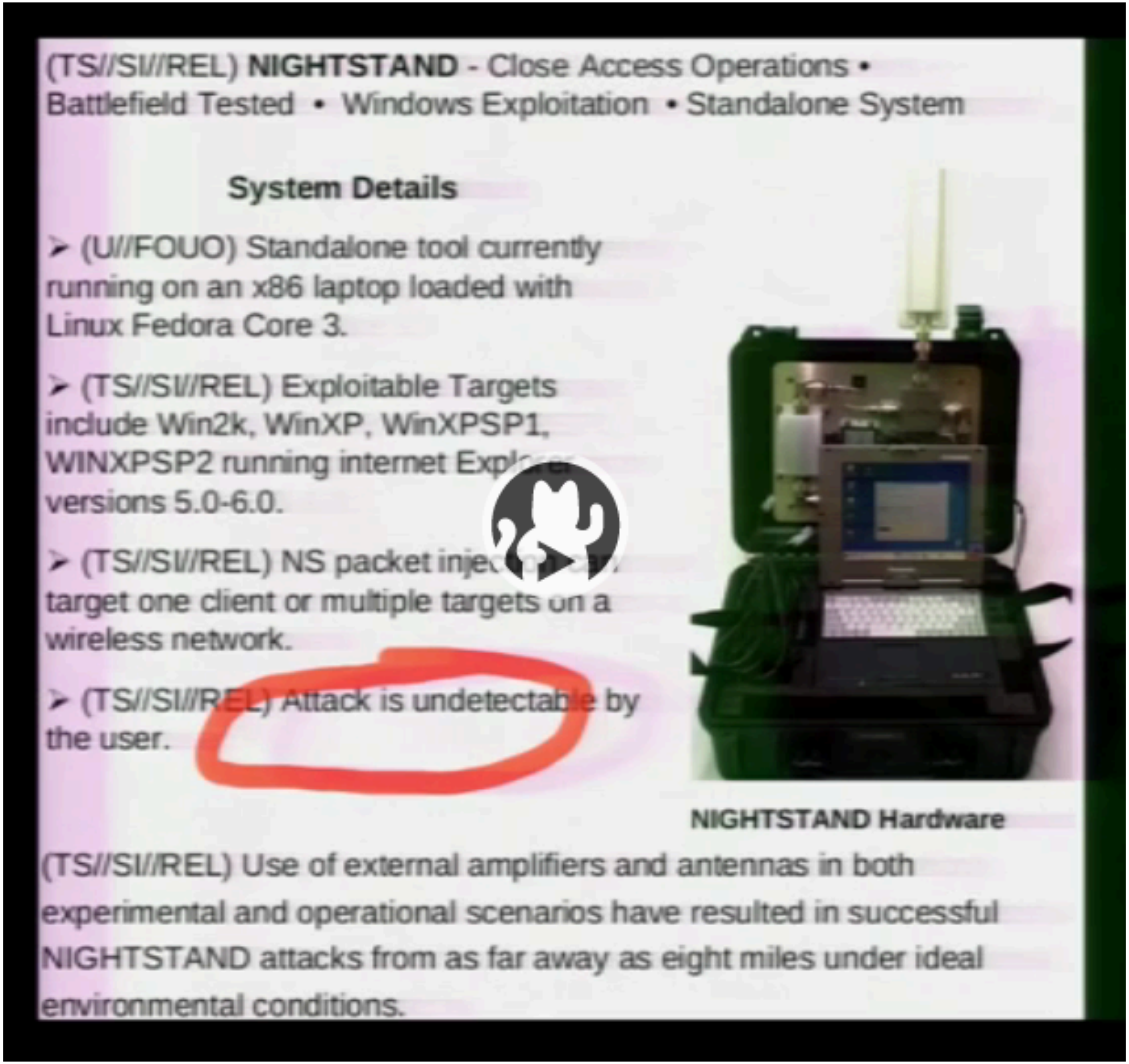
Example three: three hops away? Uh oh!
(**That's you!**)



The Big Picture

- Planetary Strategic Surveillance and...
- Exploitation Systems
- Passive sensors
- Collect (TURMOIL)
- Active attacks
- Infect (TURBINE, QFIRE, etc)
- Wait, what about "Protect?!"
- Multi-pwn!
- Blackhats used to keep your box updated
- ... these guys step on each other's toes
- Operations – “Close Access Operations“ and “Off-Net”

2013
30C3



(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

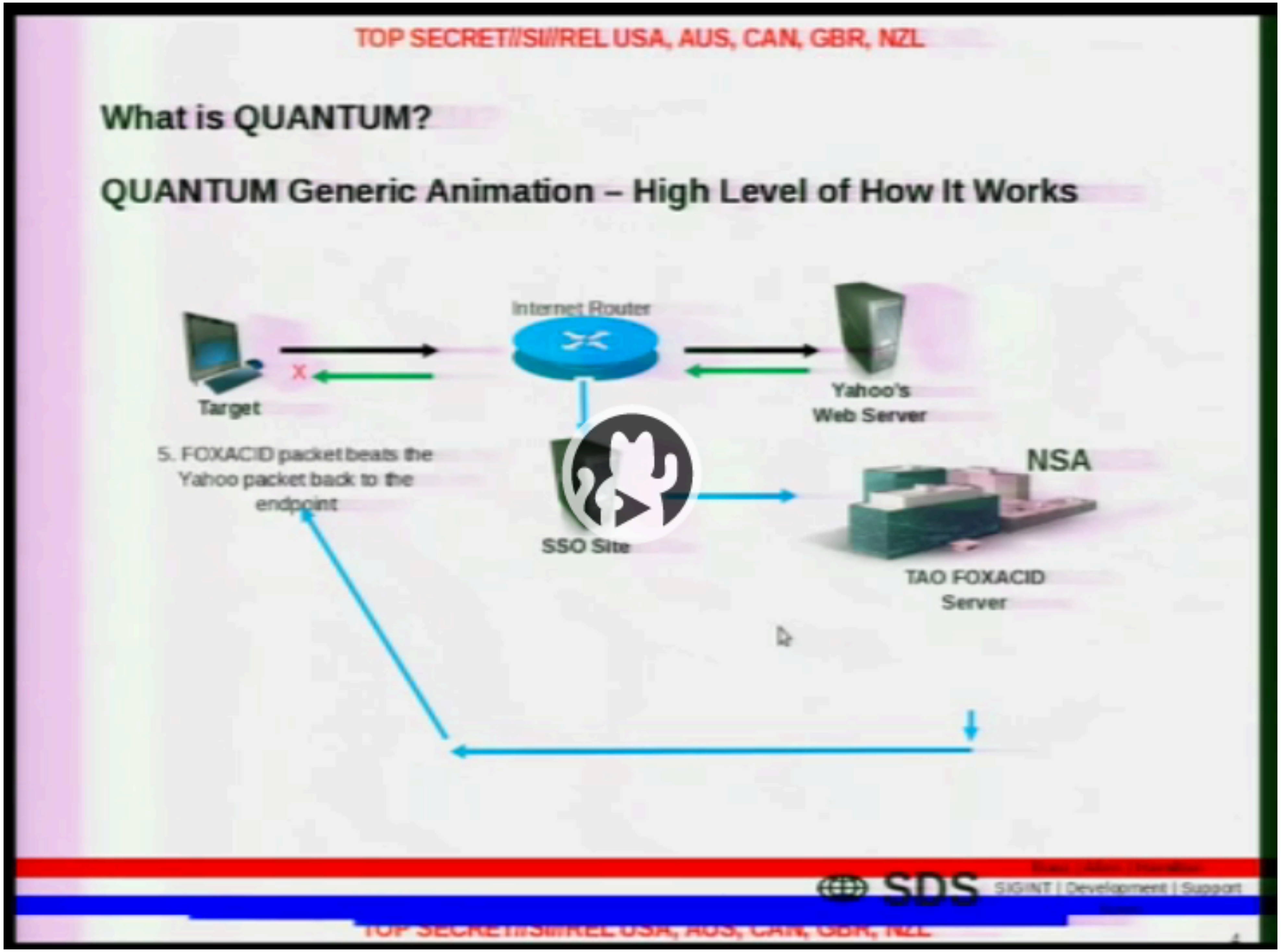
System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

2013
30C3



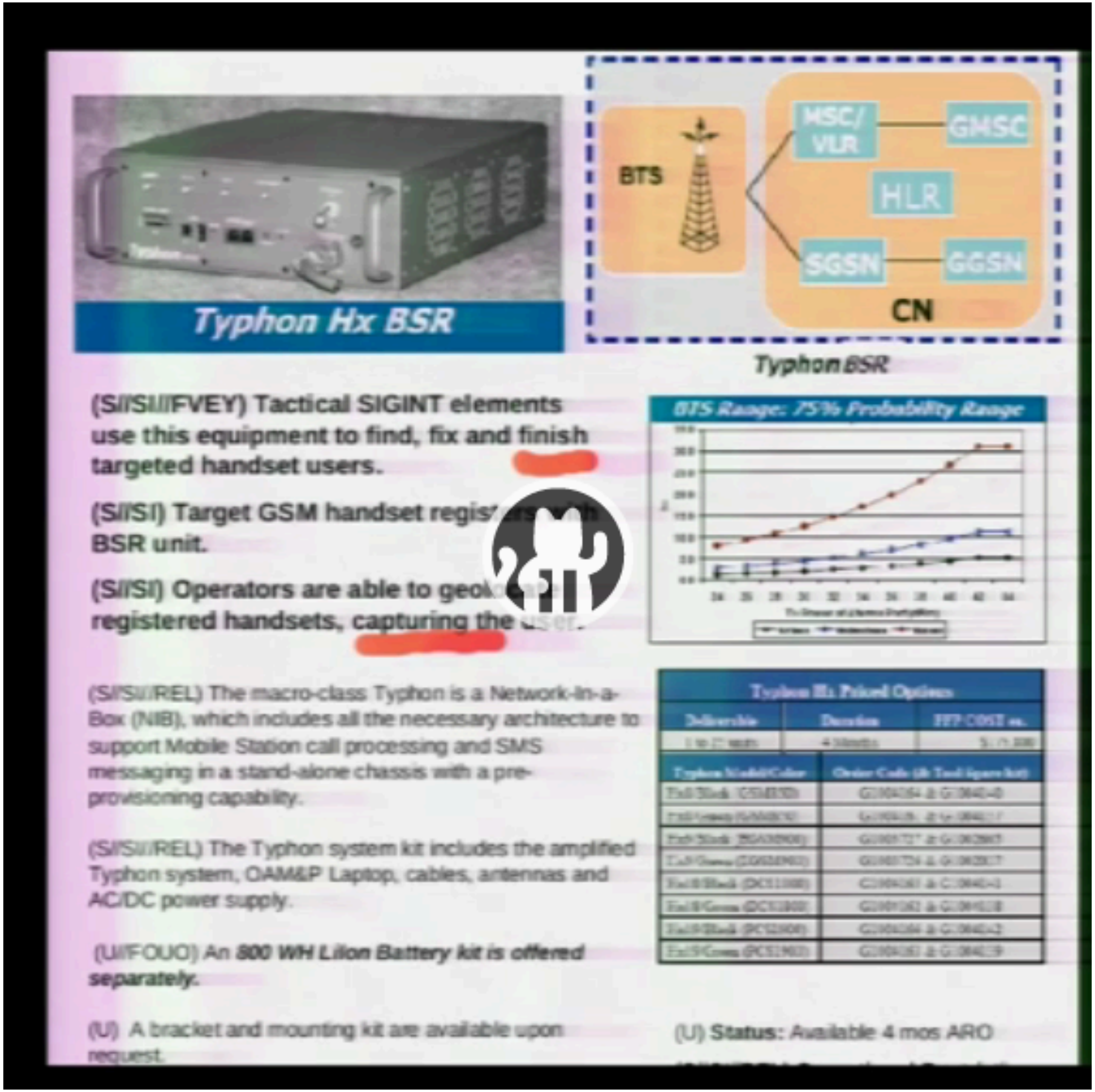
TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

Internet Router
Target
X
Yahoo's
Web Server
5. FOXACID packet beats the Yahoo packet back to the endpoint
SSO Site
NSA
TAO FOXACID
Server
SDS
SIGINT | Development | Support

TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL



Typhon BSR

(S//SI//FVEY) Tactical SIGINT elements use this equipment to find, fix and finish targeted handset users.

(S//SI) Target GSM handset registers with BSR unit.

(S//SI) Operators are able to geolocate registered handsets, capturing the user.

(S//SI//REL) The macro-class Typhon is a Network-In-a-Box (NIB), which includes all the necessary architecture to support Mobile Station call processing and SMS messaging in a stand-alone chassis with a pre-provisioning capability.

(S//SI//REL) The Typhon system kit includes the amplified Typhon system, OAM&P Laptop, cables, antennas and AC/DC power supply.

(U//FOUO) An ***800 WH LiIon Battery kit is offered separately.***

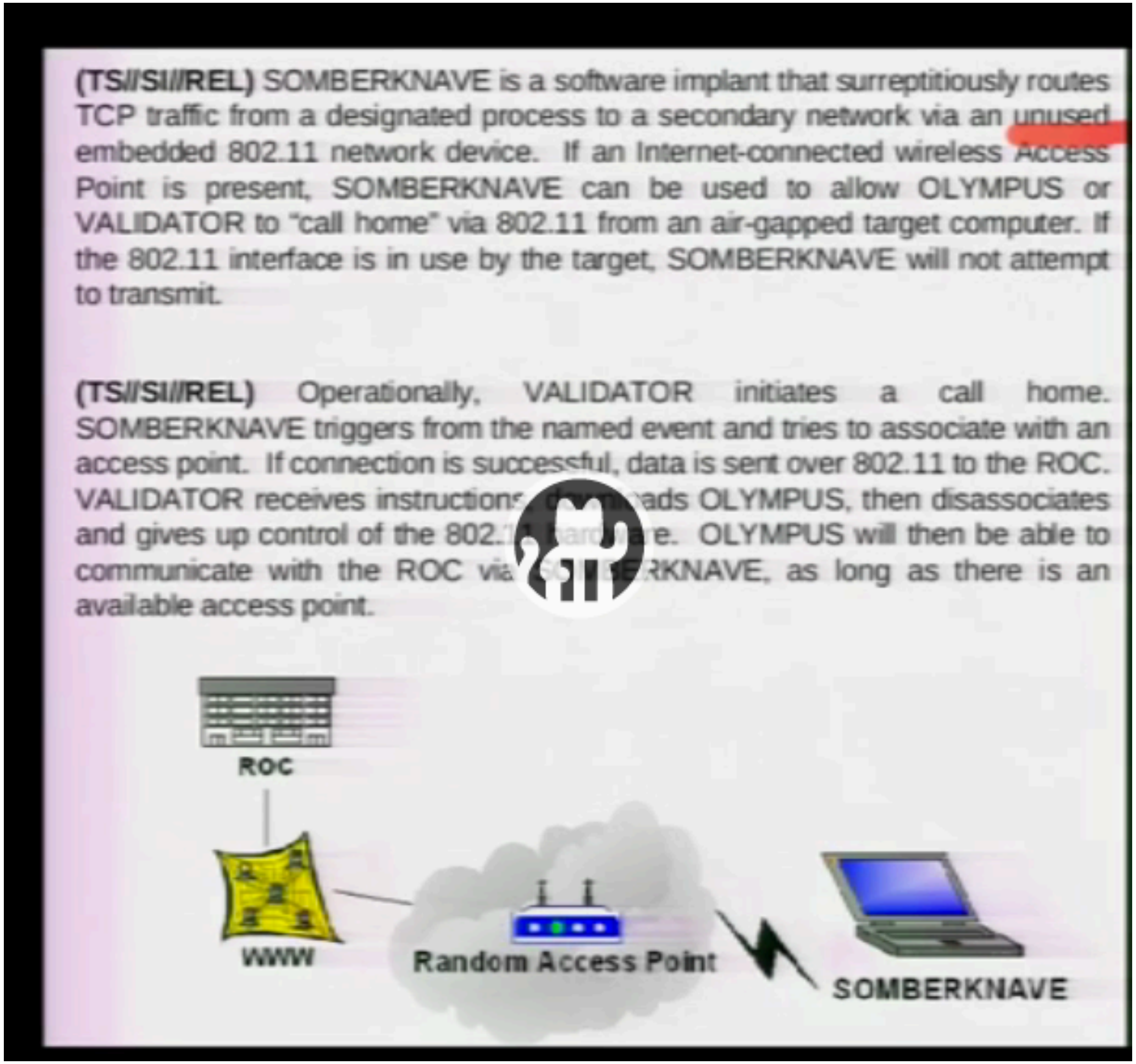
(U) A bracket and mounting kit are available upon request.

Typhon Hx Priced Options		
Deliverable	Duration	FFP COST ea.
1 to [illegible] units	4 Months	$[illegible]

Typhon Model/Color	Order Code (& Tool/spare kit)
Full Black (GSM850)	[illegible]
Full Green (GSM850)	[illegible]
Full Black (EGSM900)	[illegible]
Full Green (EGSM900)	[illegible]
Full Black (DCS1800)	[illegible]
Full Green (DCS1800)	[illegible]
Full Black (PCS1900)	[illegible]
Full Green (PCS1900)	[illegible]

(U) **Status:** Available 4 mos ARO

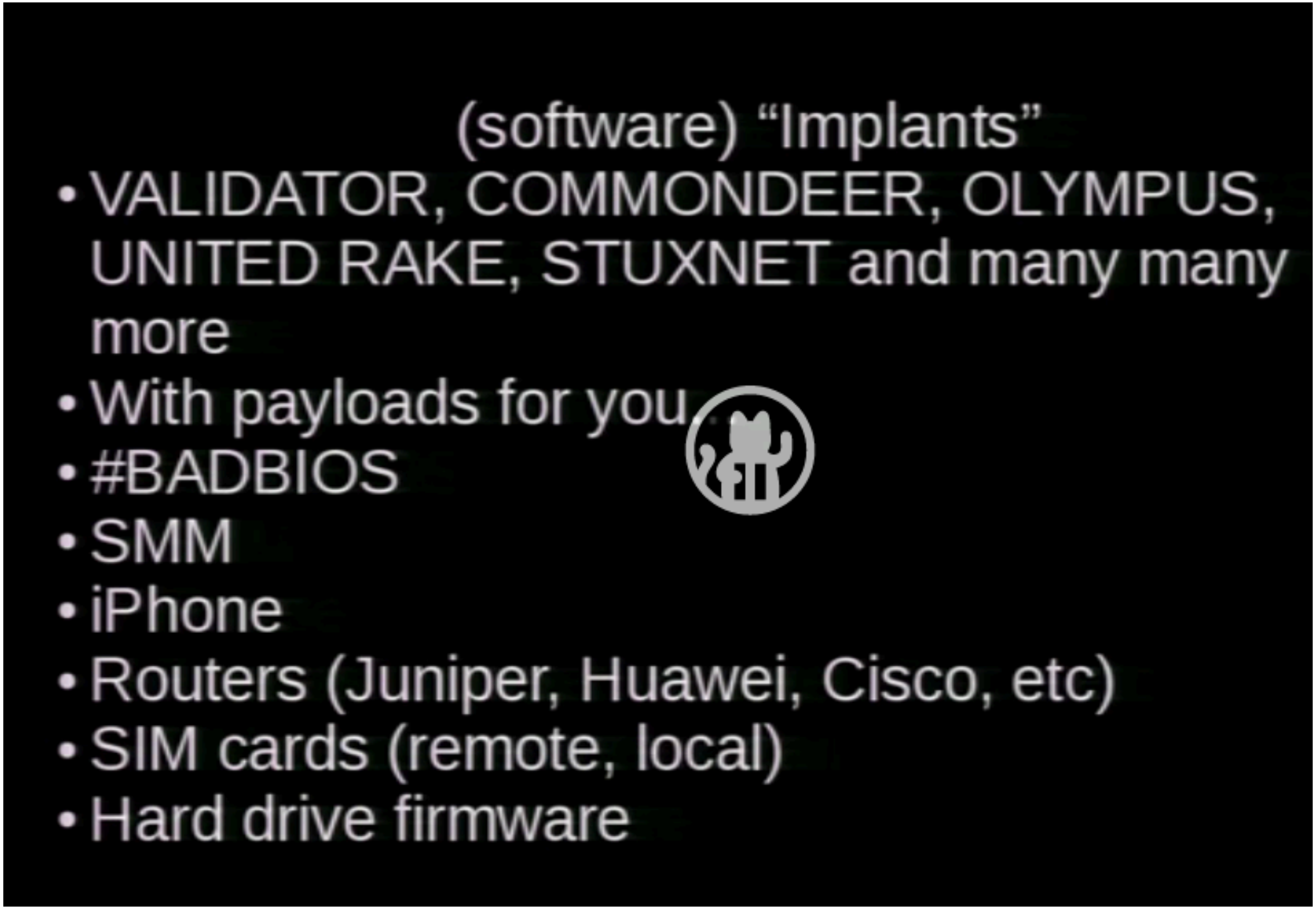
2013
30C3



(TS//SI//REL) SOMBERKNAVE is a software implant that surreptitiously routes TCP traffic from a designated process to a secondary network via an unused embedded 802.11 network device. If an Internet-connected wireless Access Point is present, SOMBERKNAVE can be used to allow OLYMPUS or VALIDATOR to "call home" via 802.11 from an air-gapped target computer. If the 802.11 interface is in use by the target, SOMBERKNAVE will not attempt to transmit.

(TS//SI//REL) Operationally, VALIDATOR initiates a call home. SOMBERKNAVE triggers from the named event and tries to associate with an access point. If connection is successful, data is sent over 802.11 to the ROC. VALIDATOR receives instructions, downloads OLYMPUS, then disassociates and gives up control of the 802.11 hardware. OLYMPUS will then be able to communicate with the ROC via SOMBERKNAVE, as long as there is an available access point.

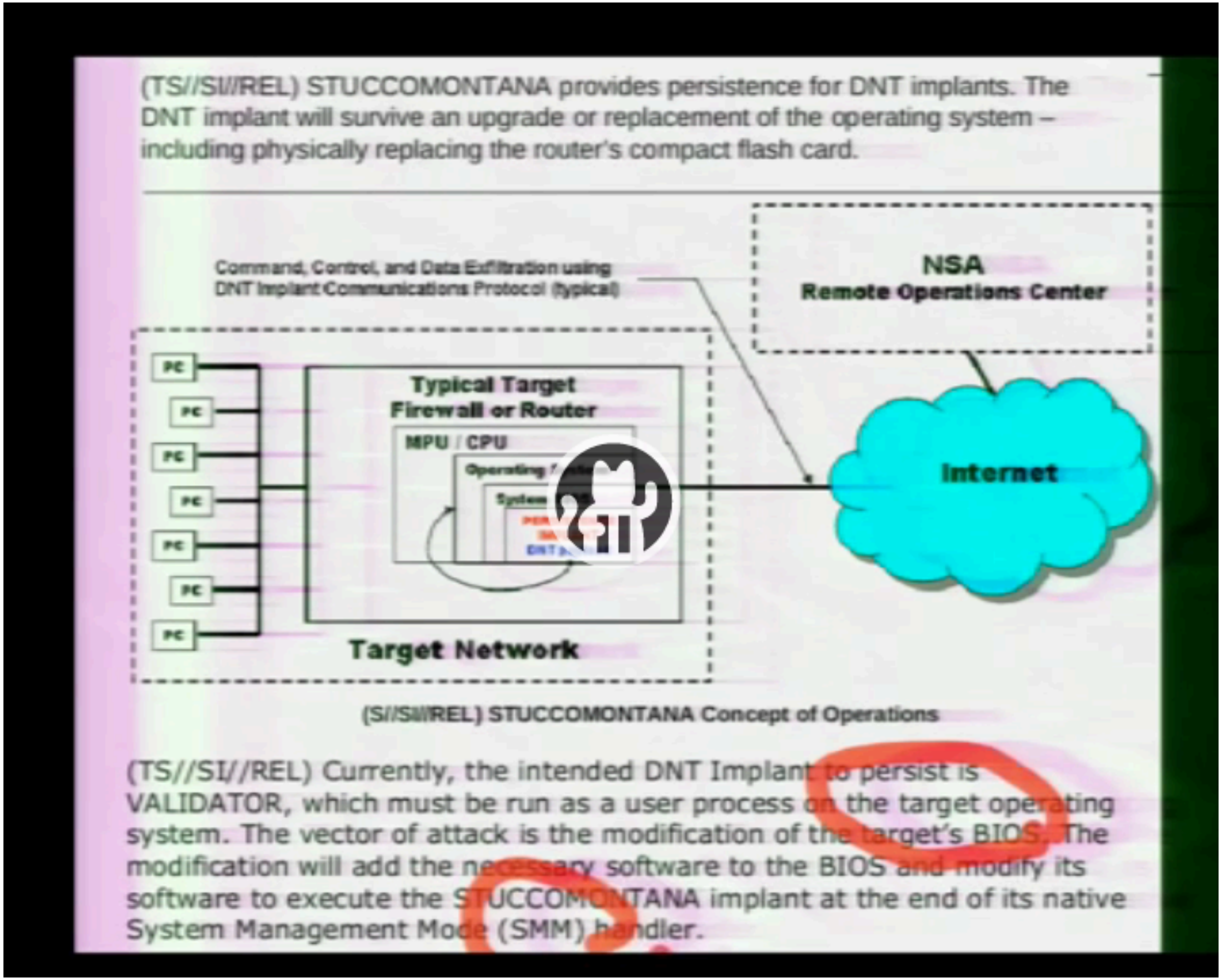
2013
30C3



(software) “Implants”

- VALIDATOR, COMMONDEER, OLYMPUS, UNITED RAKE, STUXNET and many many more
- With payloads for you...
- #BADBIOS
- SMM
- iPhone
- Routers (Juniper, Huawei, Cisco, etc)
- SIM cards (remote, local)
- Hard drive firmware

2013
30C3

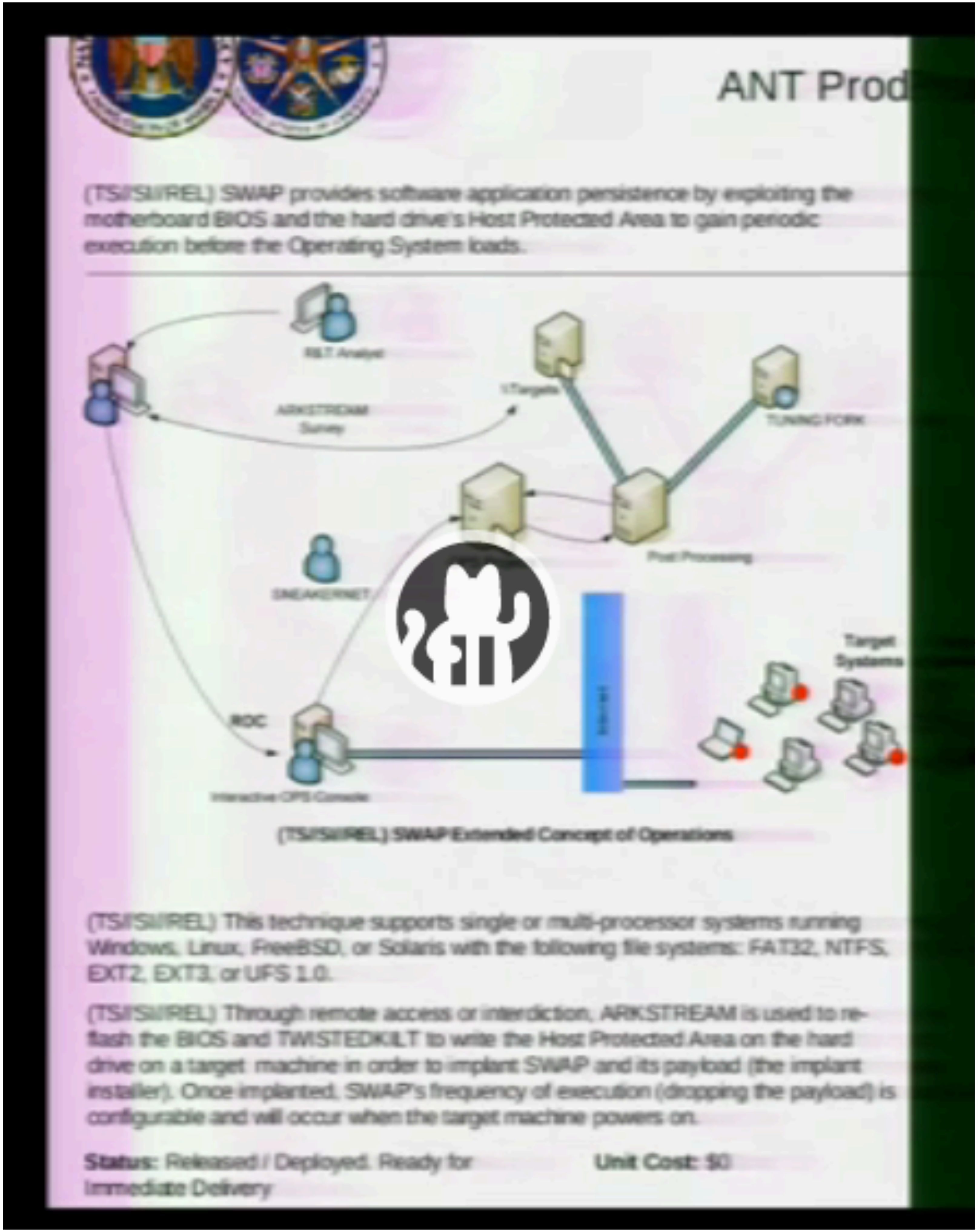


(TS//SI//REL) STUCCOMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.

(S//SI//REL) STUCCOMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the STUCCOMONTANA implant at the end of its native System Management Mode (SMM) handler.

2013
30C3



ANT Prod

(TS//SI//REL) SWAP provides software application persistence by exploiting the motherboard BIOS and the hard drive's Host Protected Area to gain periodic execution before the Operating System loads.

(TS//SI//REL) SWAP Extended Concept of Operations

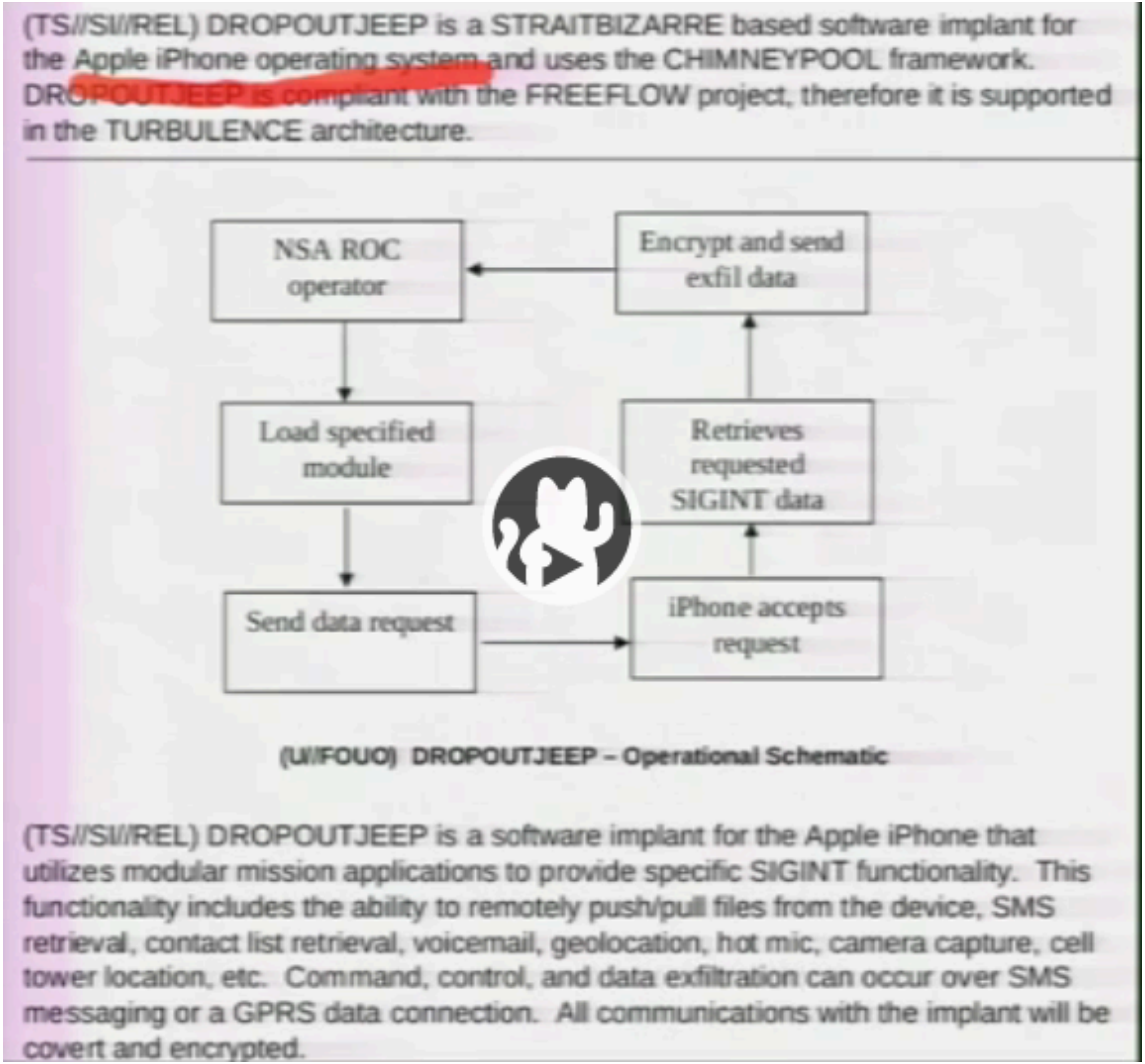
(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

2013
30C3



(TS//SI//REL) DROPOUTJEEP is a STRAITBIZARRE based software implant for the Apple iPhone operating system and uses the CHIMNEYPOOL framework. DROPOUTJEEP is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

NSA ROC operator

Load specified module

Send data request

iPhone accepts request

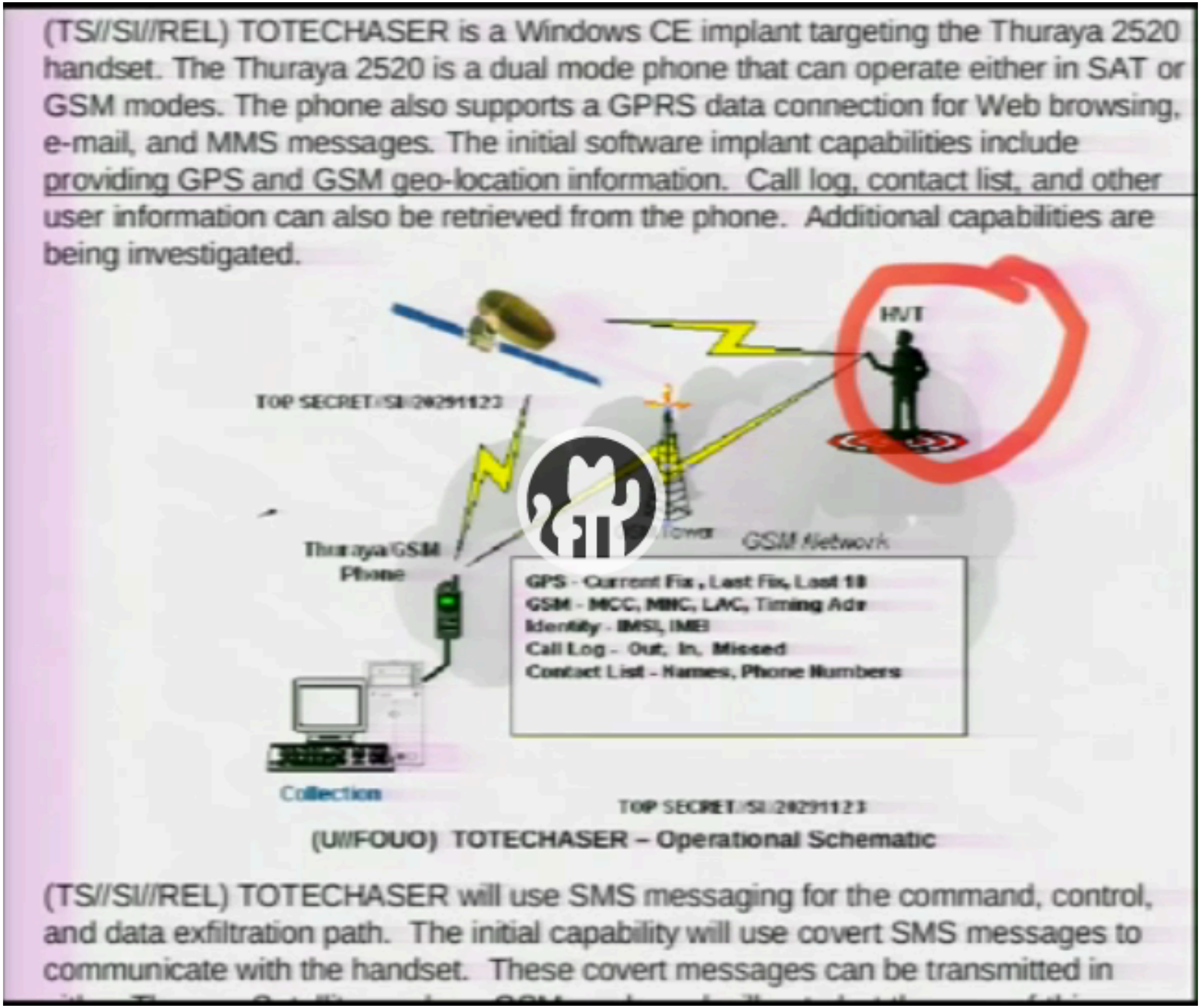
Retrieves requested SIGINT data

Encrypt and send exfil data

(U//FOUO) DROPOUTJEEP – Operational Schematic

(TS//SI//REL) DROPOUTJEEP is a software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted.

2013
30C3



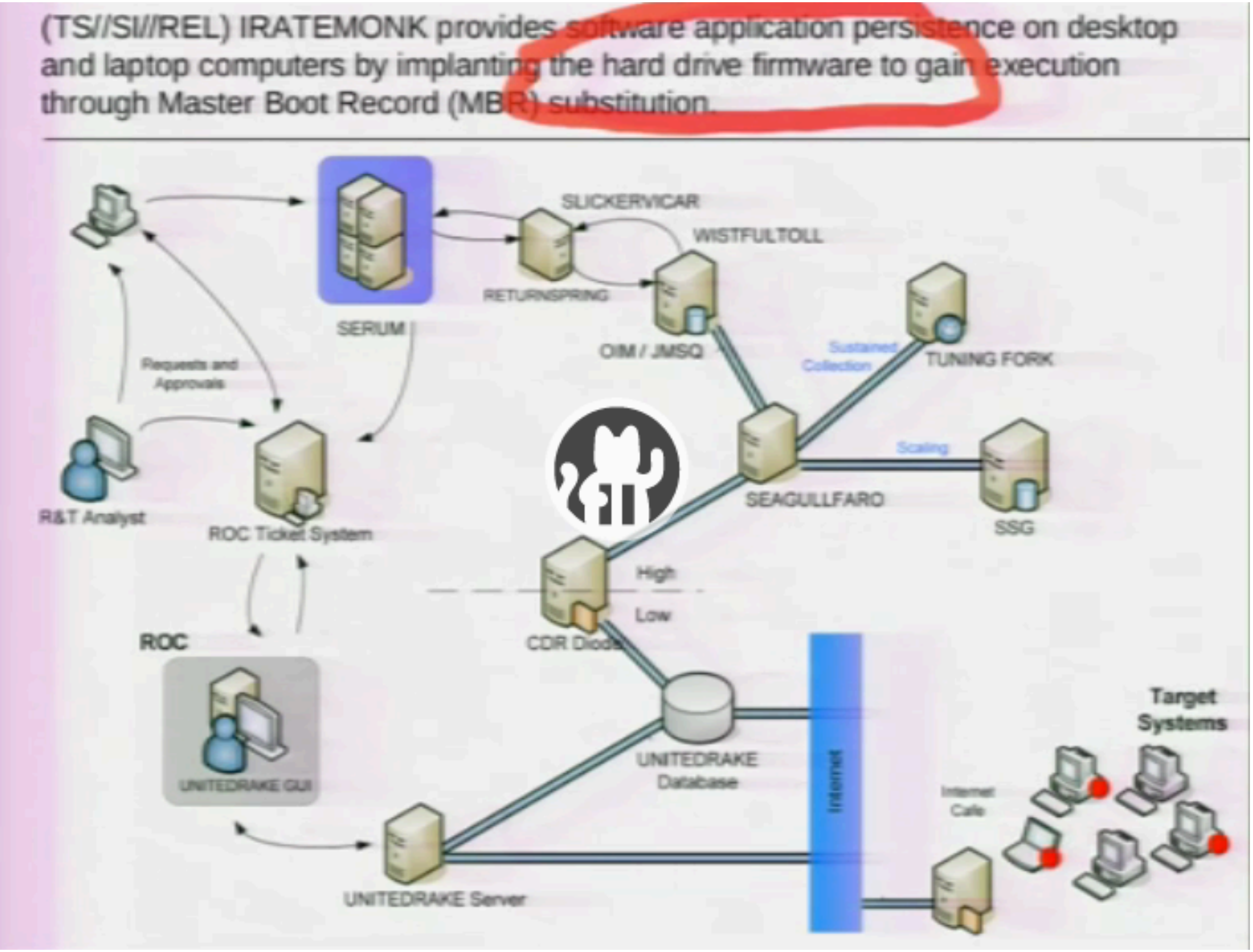
(TS//SI//REL) TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. The Thuraya 2520 is a dual mode phone that can operate either in SAT or GSM modes. The phone also supports a GPRS data connection for Web browsing, e-mail, and MMS messages. The initial software implant capabilities include providing GPS and GSM geo-location information. Call log, contact list, and other user information can also be retrieved from the phone. Additional capabilities are being investigated.

GPS - Current Fix , Last Fix, Last 10
GSM - MCC, MNC, LAC, Timing Adv
Identity - IMSI, IMEI
Call Log - Out, In, Missed
Contact List - Names, Phone Numbers

(U//FOUO) TOTECHASER – Operational Schematic

(TS//SI//REL) TOTECHASER will use SMS messaging for the command, control, and data exfiltration path. The initial capability will use covert SMS messages to communicate with the handset. These covert messages can be transmitted in

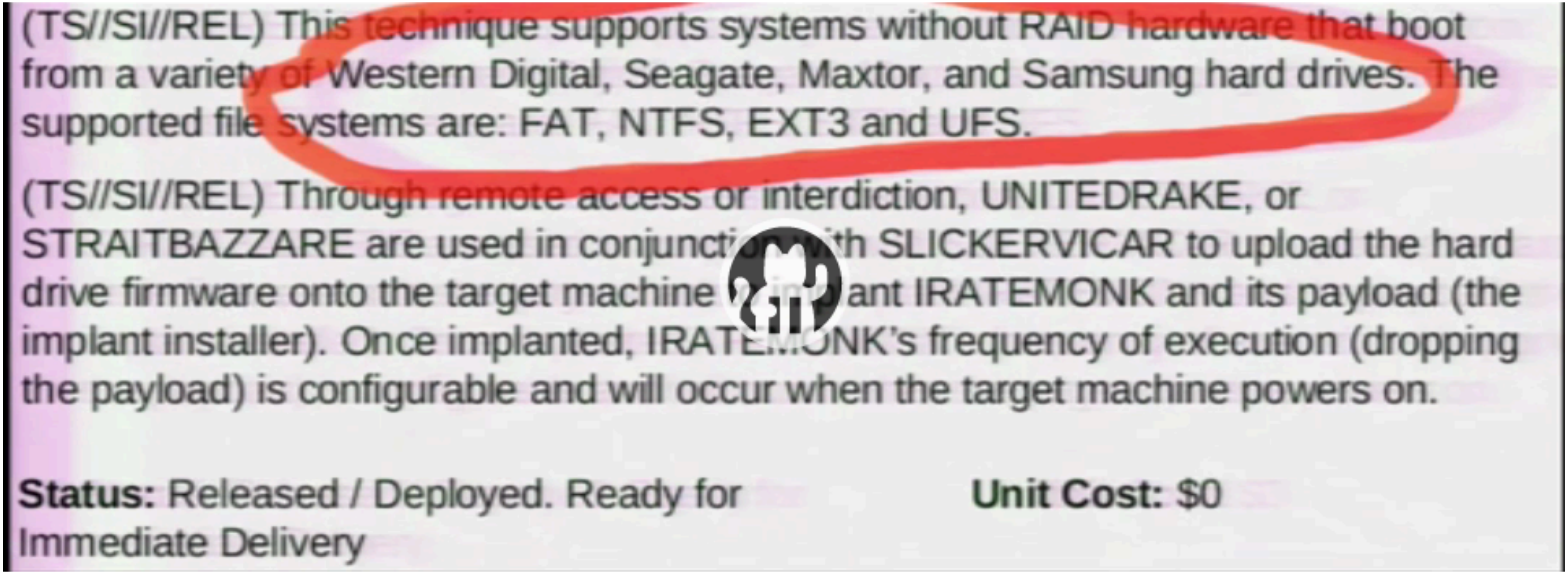
2013
30C3



(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.

2013

30C3



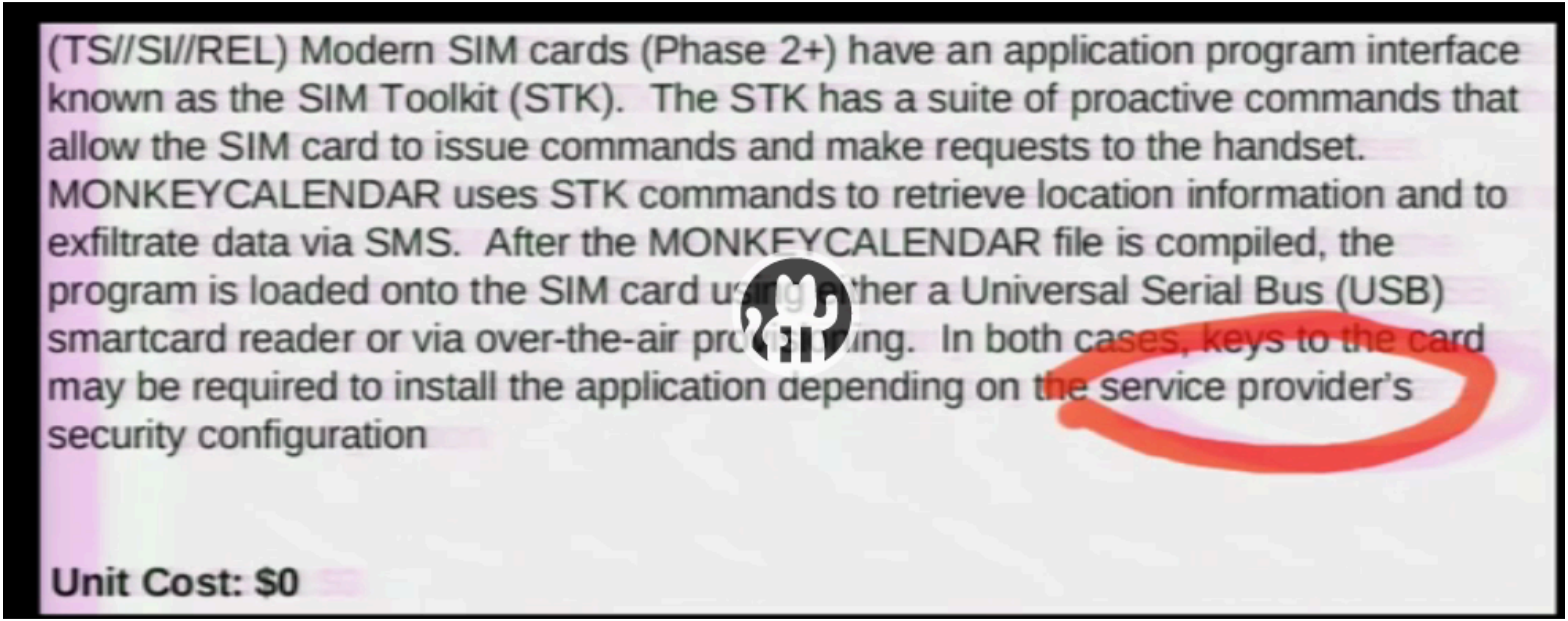
(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: $0

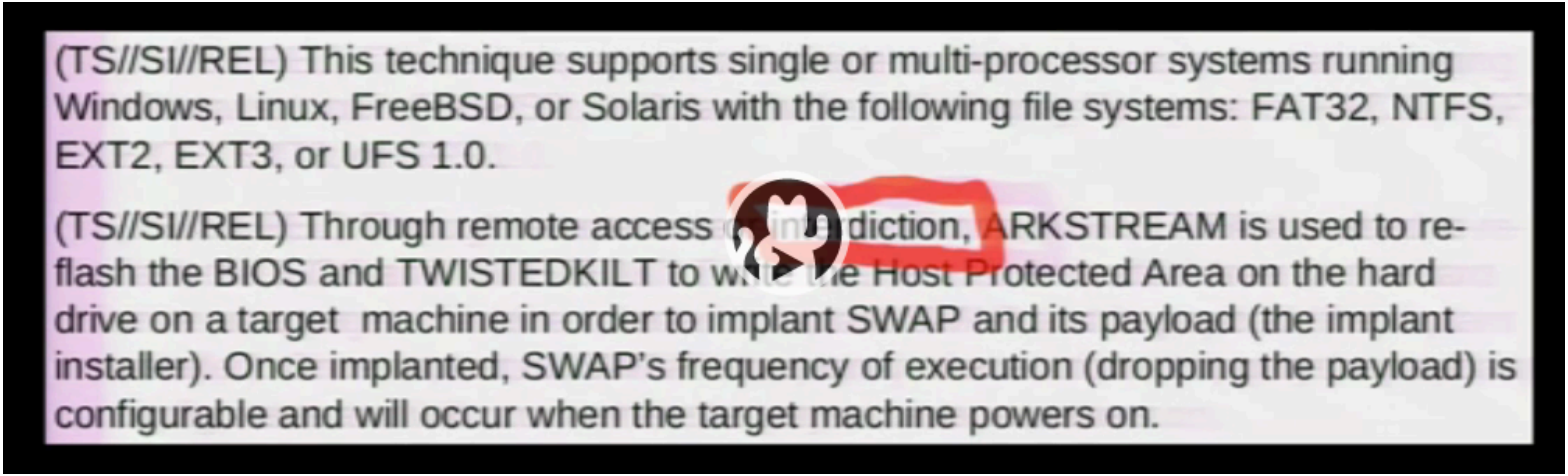
2013
30C3



(TS//SI//REL) Modern SIM cards (Phase 2+) have an application program interface known as the SIM Toolkit (STK). The STK has a suite of proactive commands that allow the SIM card to issue commands and make requests to the handset. MONKEYCALENDAR uses STK commands to retrieve location information and to exfiltrate data via SMS. After the MONKEYCALENDAR file is compiled, the program is loaded onto the SIM card using either a Universal Serial Bus (USB) smartcard reader or via over-the-air provisioning. In both cases, keys to the card may be required to install the application depending on the service provider's security configuration

Unit Cost: $0

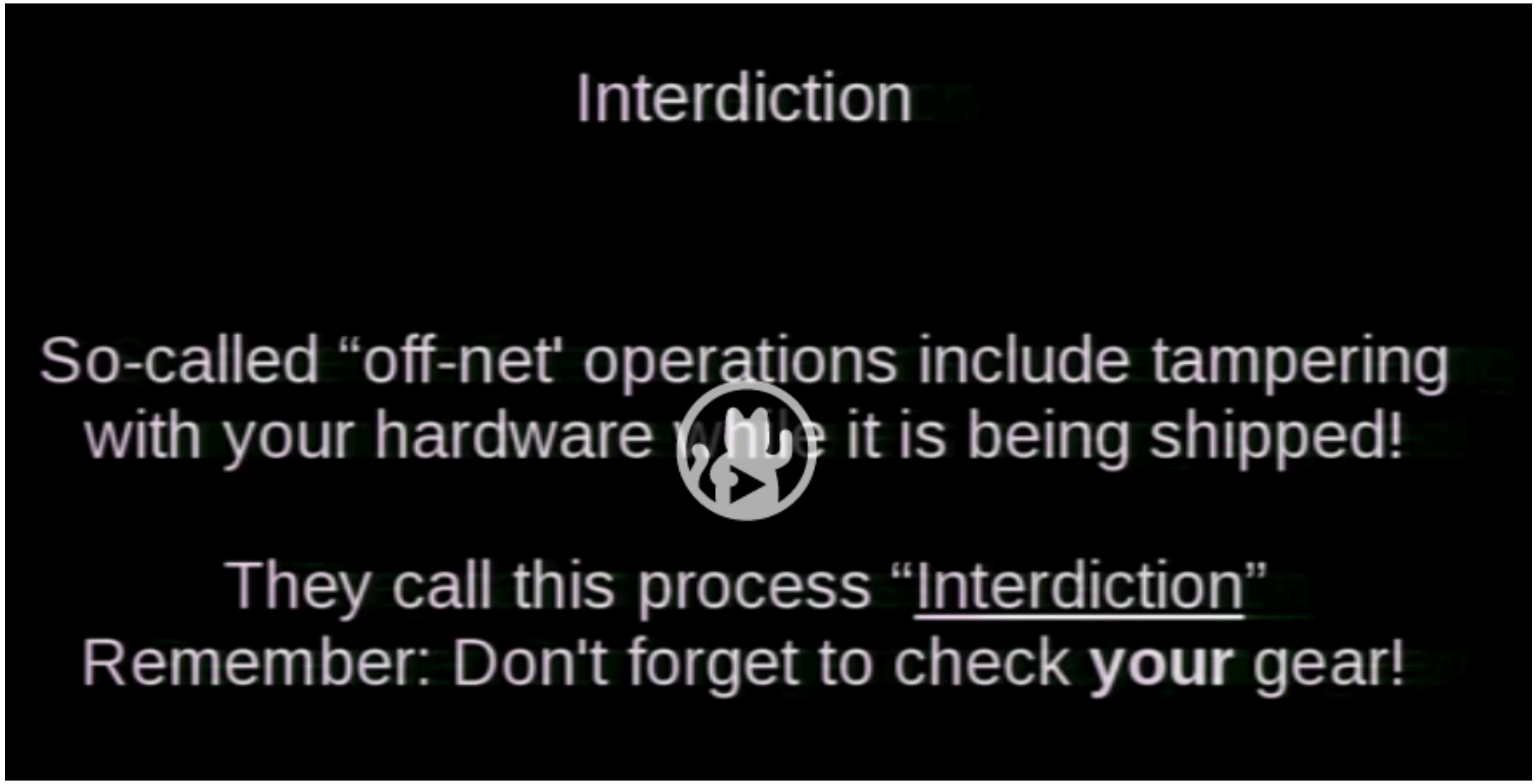
2013
30C3



(TS//SI//REL) This technique supports single or multi-processor systems running Windows, Linux, FreeBSD, or Solaris with the following file systems: FAT32, NTFS, EXT2, EXT3, or UFS 1.0.

(TS//SI//REL) Through remote access or interdiction, ARKSTREAM is used to re-flash the BIOS and TWISTEDKILT to write the Host Protected Area on the hard drive on a target machine in order to implant SWAP and its payload (the implant installer). Once implanted, SWAP's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

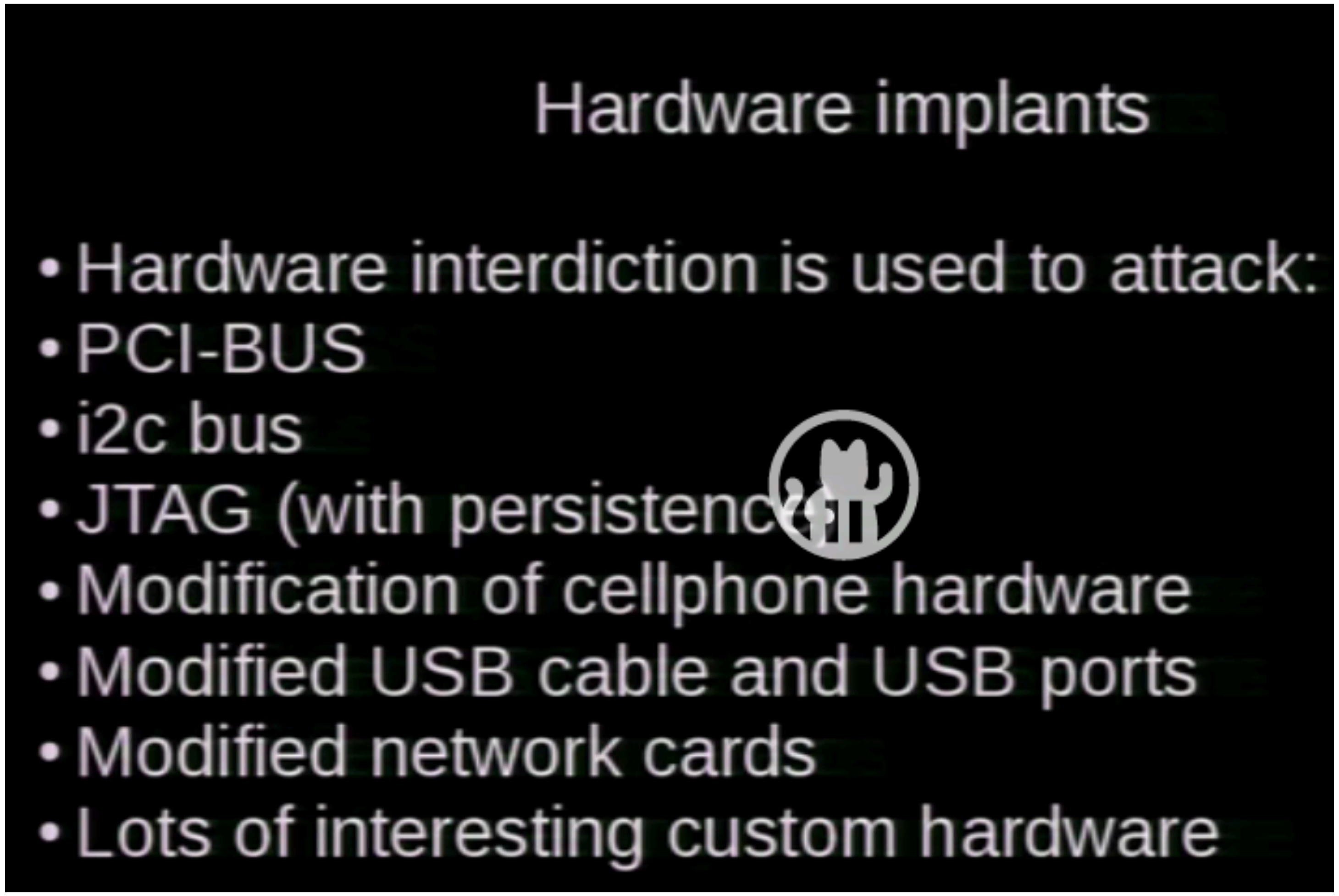
2013
30C3



Interdiction

So-called “off-net' operations include tampering with your hardware while it is being shipped!

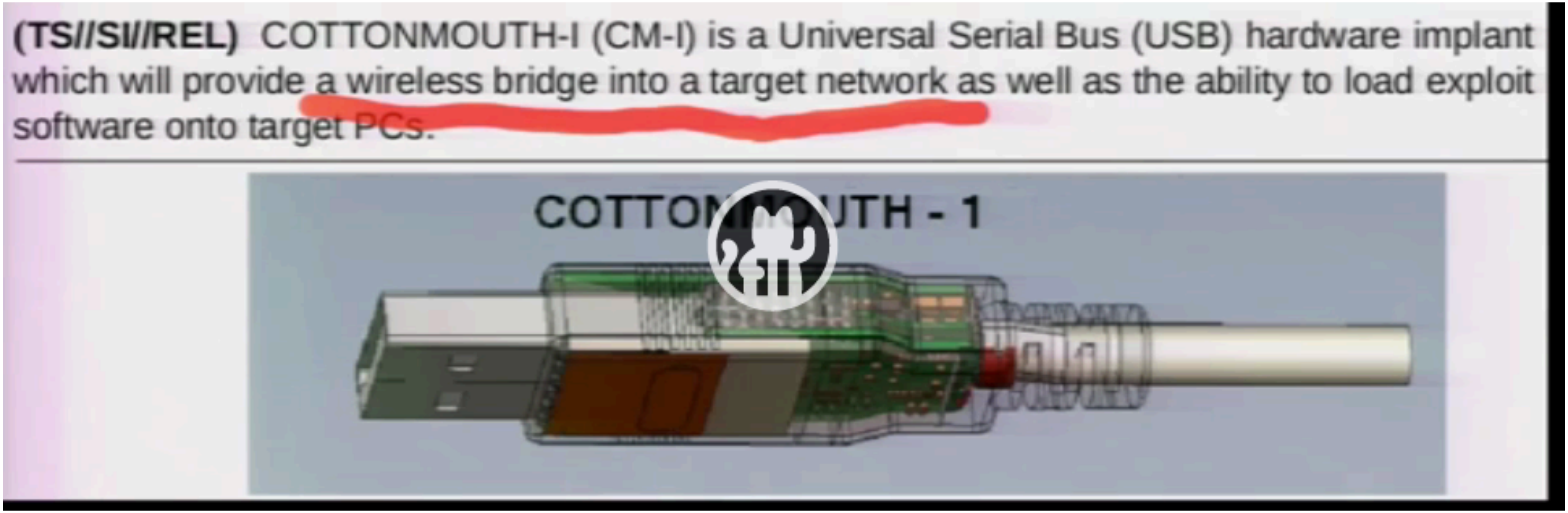
They call this process “Interdiction”
Remember: Don't forget to check **your** gear!



Hardware implants

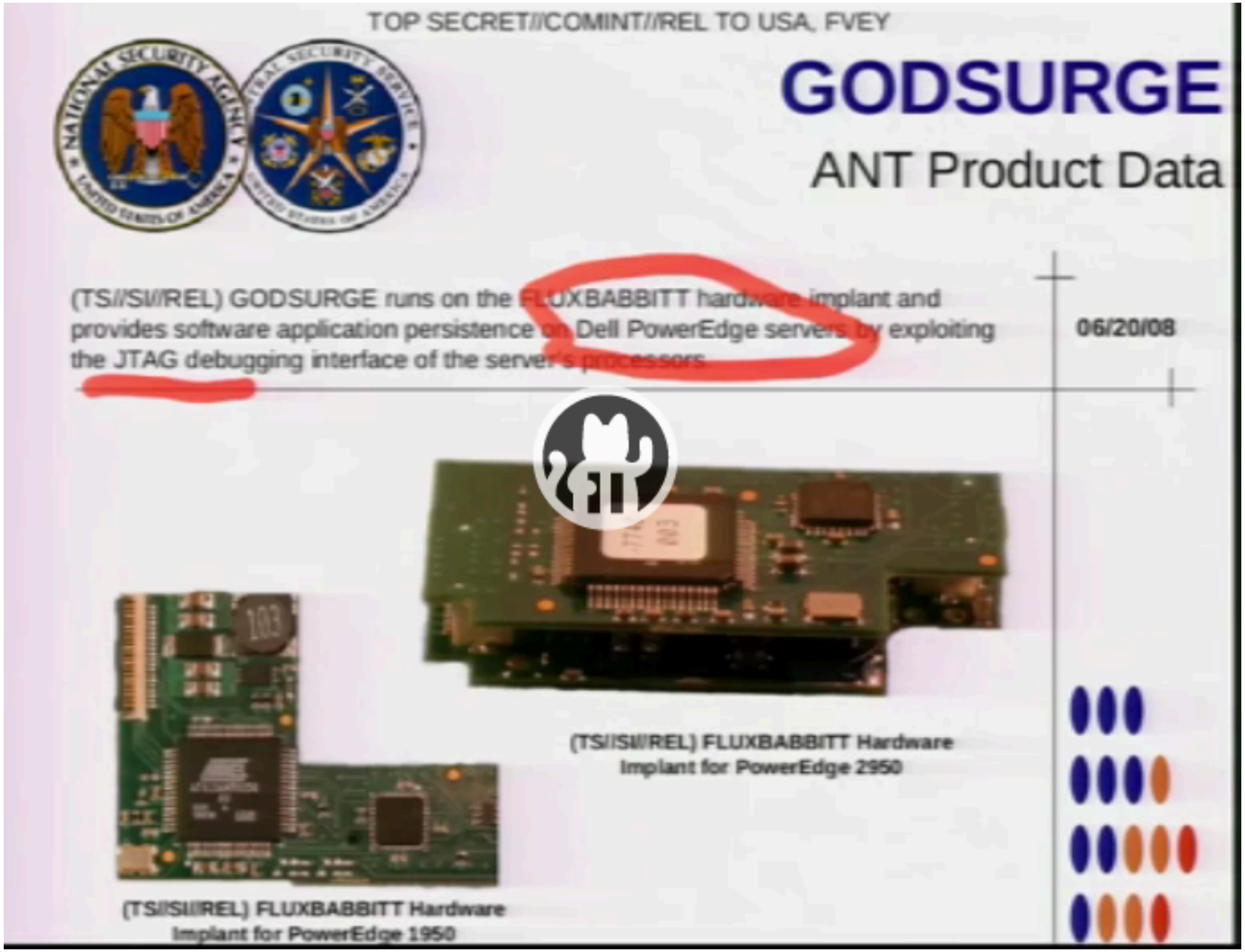
- Hardware interdiction is used to attack:
- PCI-BUS
- i2c bus
- JTAG (with persistence)
- Modification of cellphone hardware
- Modified USB cable and USB ports
- Modified network cards
- Lots of interesting custom hardware

2013
30C3



(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.

2013
30C3



TOP SECRET//COMINT//REL TO USA, FVEY

GODSURGE

ANT Product Data

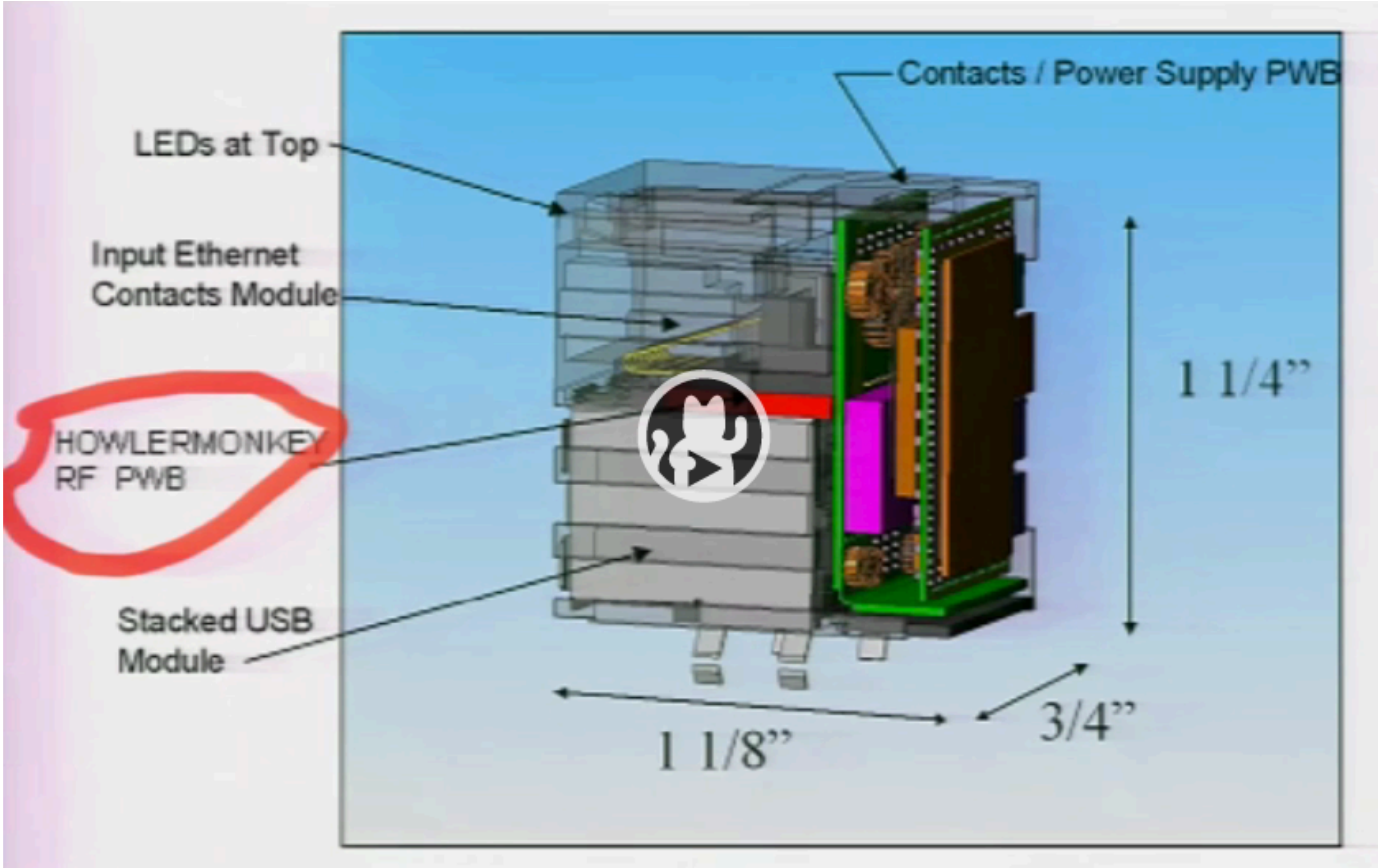
(TS//SI//REL) GODSURGE runs on the FLUXBABBITT hardware implant and provides software application persistence on Dell PowerEdge servers by exploiting the JTAG debugging interface of the server's processors.

06/20/08

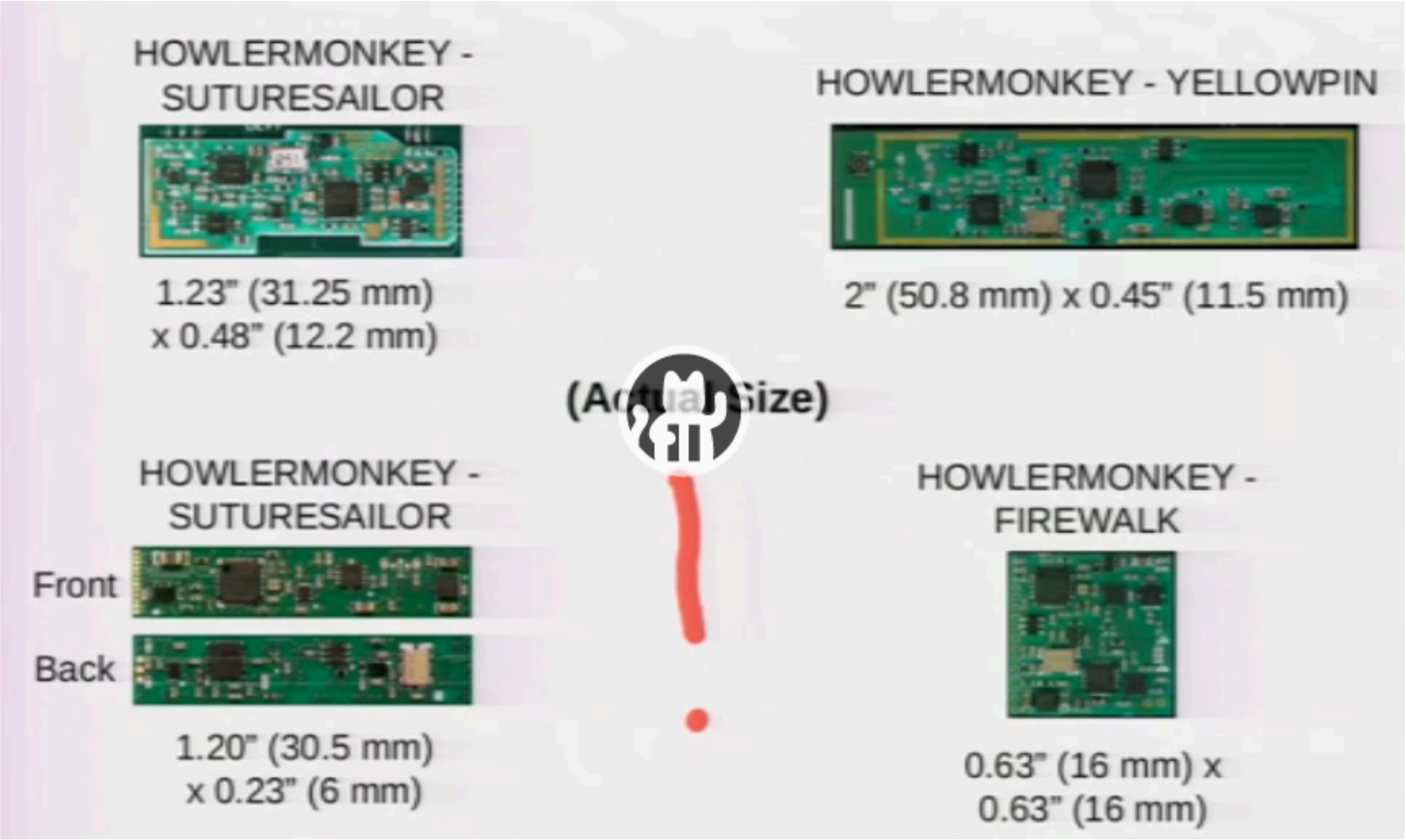
(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 2950

(TS//SI//REL) FLUXBABBITT Hardware Implant for PowerEdge 1950

2013
30C3


Contacts / Power Supply PWB
LEDs at Top
Input Ethernet
Contacts Module
HOWLERMONKEY
RF PWB
Stacked USB
Module
1 1/4”
1 1/8”
3/4”

2013
30C3



HOWLERMONKEY - SUTURESAILOR

1.23" (31.25 mm) x 0.48" (12.2 mm)

HOWLERMONKEY - YELLOWPIN

2" (50.8 mm) x 0.45" (11.5 mm)

(Actual Size)

HOWLERMONKEY - SUTURESAILOR

Front

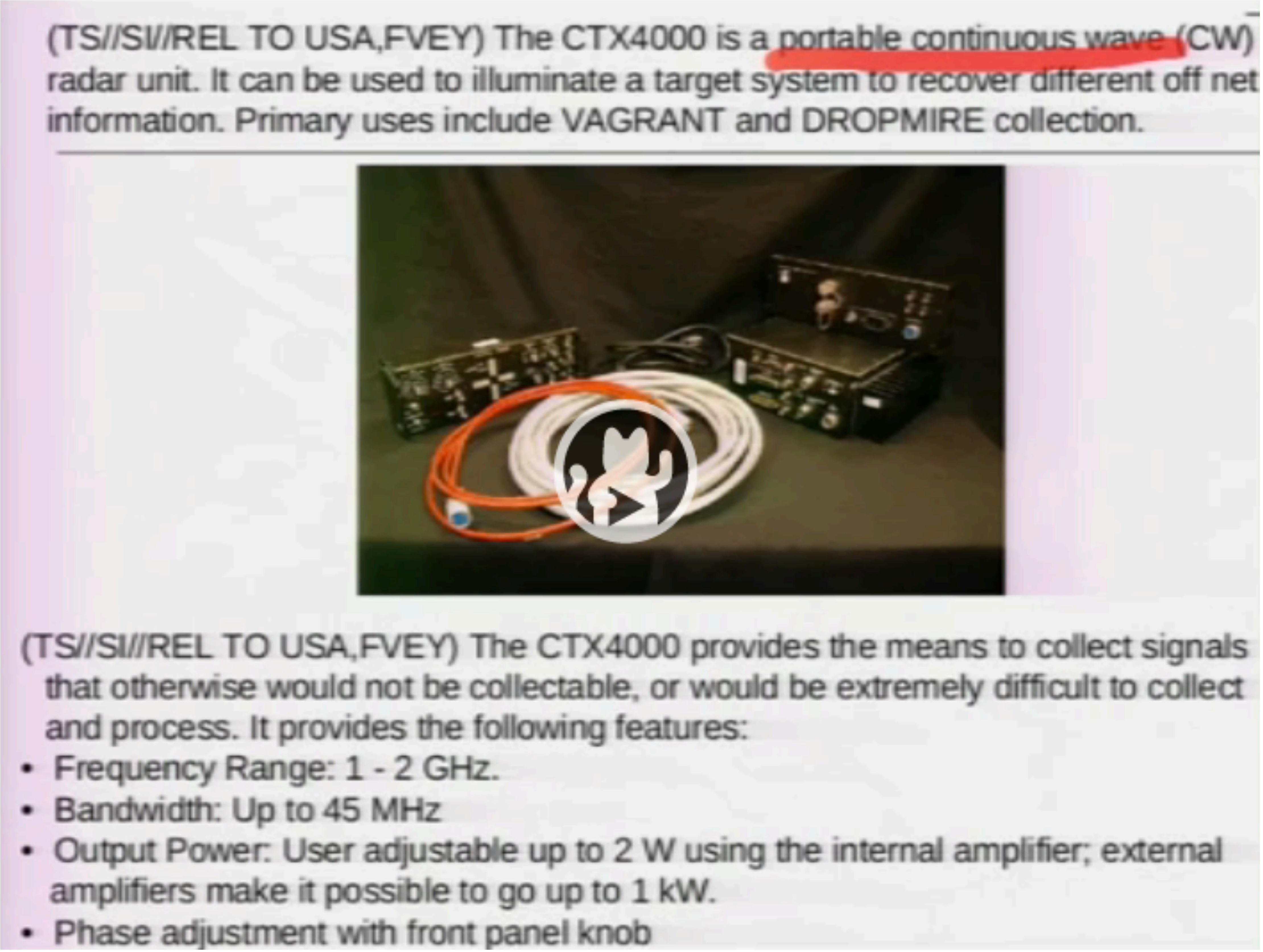
Back

1.20" (30.5 mm) x 0.23" (6 mm)

HOWLERMONKEY - FIREWALK

0.63" (16 mm) x 0.63" (16 mm)

2013
30C3

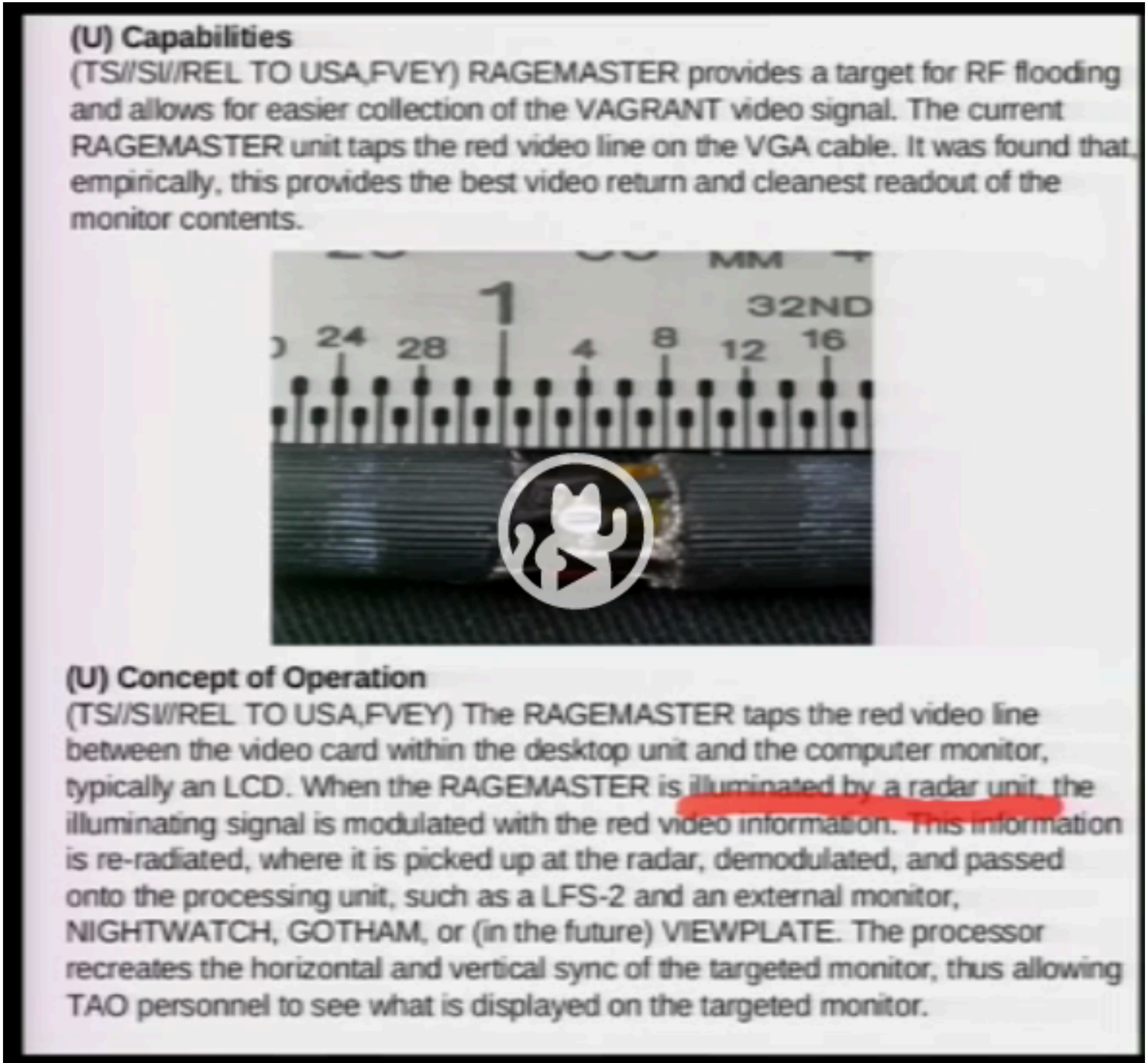


(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob

2013
30C3



(U) Capabilities

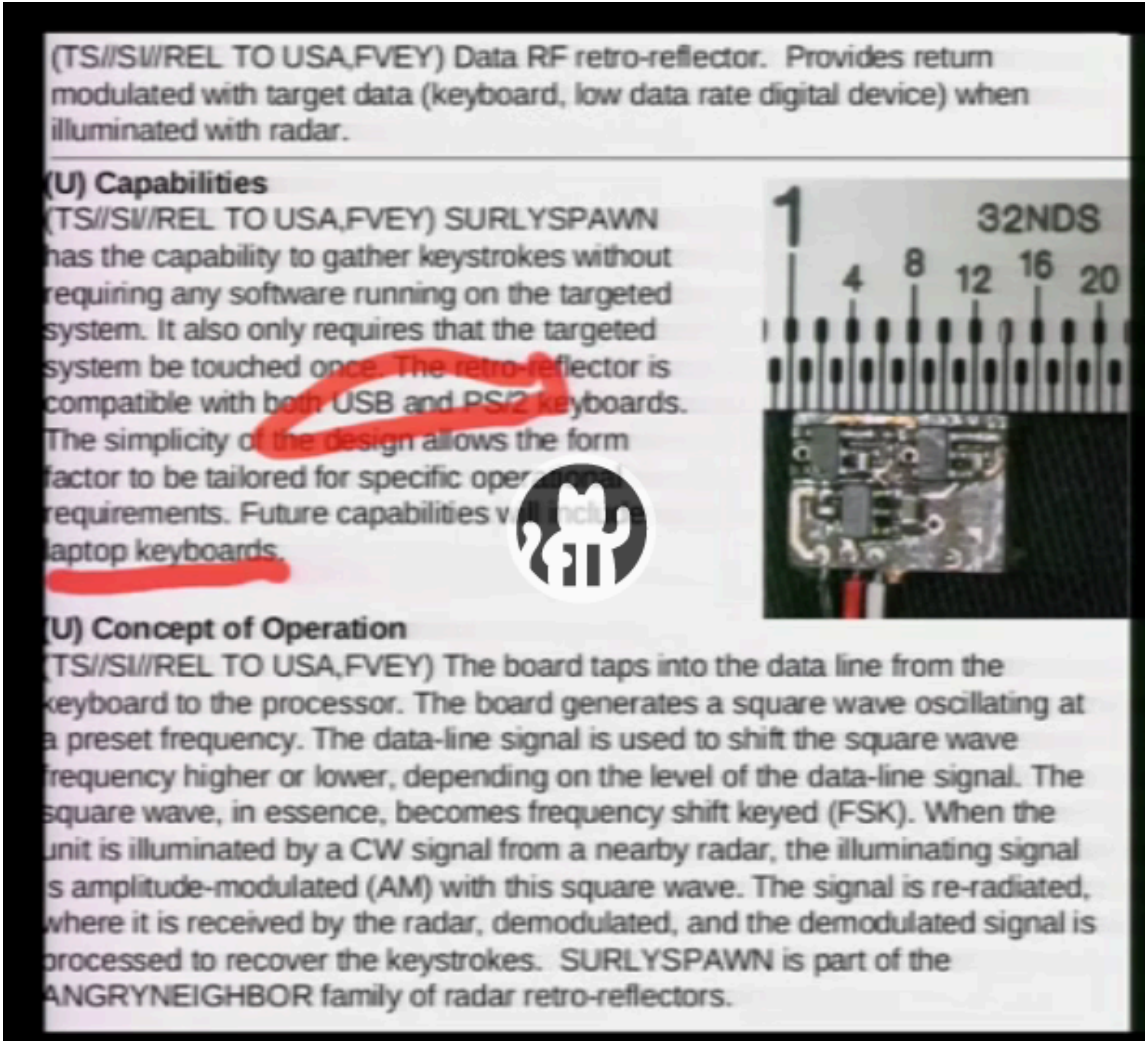
(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.

MM
1
32ND
24
28
4
8
12
16

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

2013
30C3



(TS//SI//REL TO USA,FVEY) Data RF retro-reflector. Provides return modulated with target data (keyboard, low data rate digital device) when illuminated with radar.

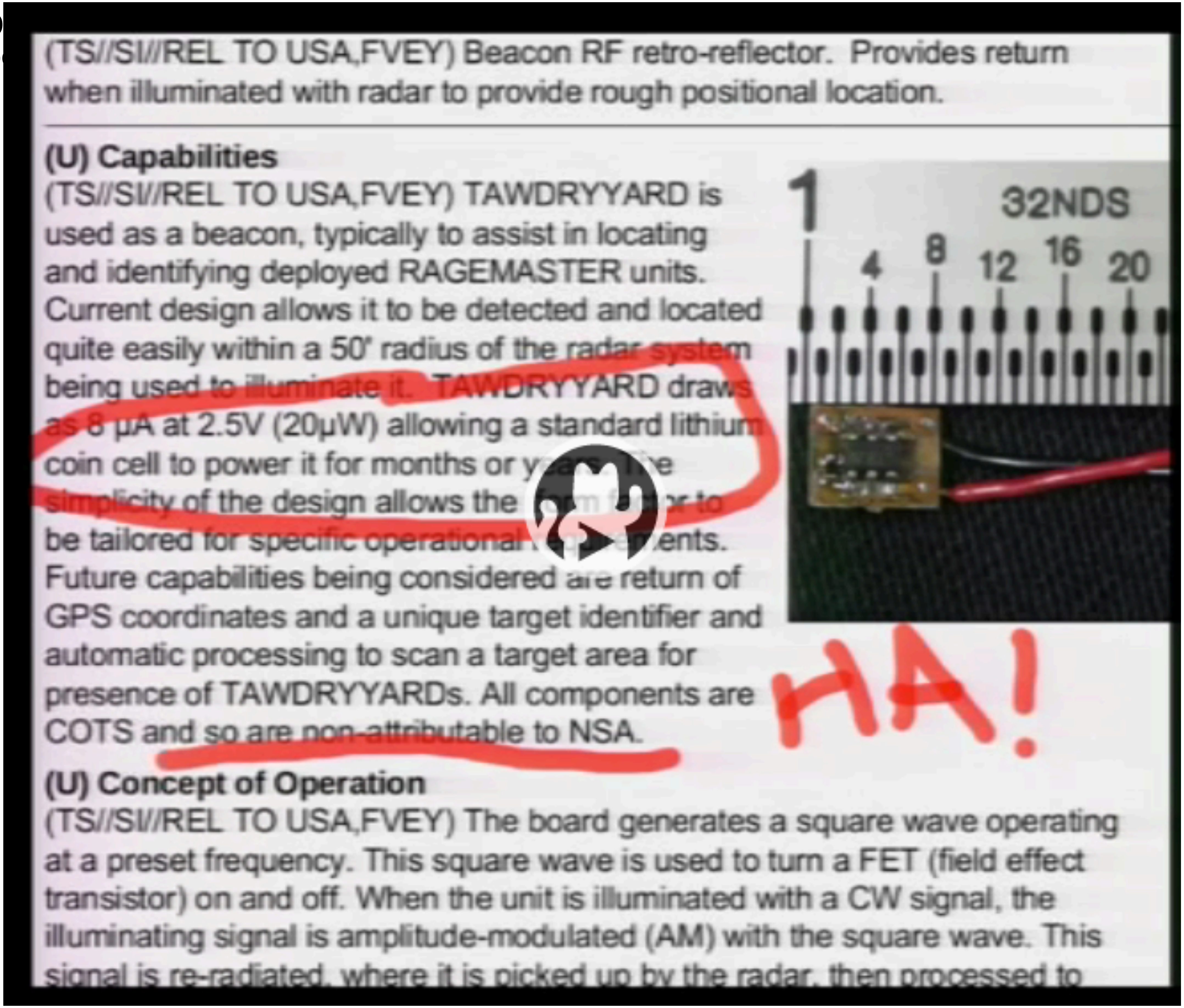
(U) Capabilities

(TS//SI//REL TO USA,FVEY) SURLYSPAWN has the capability to gather keystrokes without requiring any software running on the targeted system. It also only requires that the targeted system be touched once. The retro-reflector is compatible with both USB and PS/2 keyboards. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities will include laptop keyboards.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board taps into the data line from the keyboard to the processor. The board generates a square wave oscillating at a preset frequency. The data-line signal is used to shift the square wave frequency higher or lower, depending on the level of the data-line signal. The square wave, in essence, becomes frequency shift keyed (FSK). When the unit is illuminated by a CW signal from a nearby radar, the illuminating signal is amplitude-modulated (AM) with this square wave. The signal is re-radiated, where it is received by the radar, demodulated, and the demodulated signal is processed to recover the keystrokes. SURLYSPAWN is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

20
30



(TS//SI//REL TO USA,FVEY) Beacon RF retro-reflector. Provides return when illuminated with radar to provide rough positional location.

(U) Capabilities

(TS//SI//REL TO USA,FVEY) TAWDRYYARD is used as a beacon, typically to assist in locating and identifying deployed RAGEMASTER units. Current design allows it to be detected and located quite easily within a 50' radius of the radar system being used to illuminate it. TAWDRYYARD draws as 8 µA at 2.5V (20µW) allowing a standard lithium coin cell to power it for months or years. The simplicity of the design allows the form factor to be tailored for specific operational requirements. Future capabilities being considered are return of GPS coordinates and a unique target identifier and automatic processing to scan a target area for presence of TAWDRYYARDs. All components are COTS and so are non-attributable to NSA.

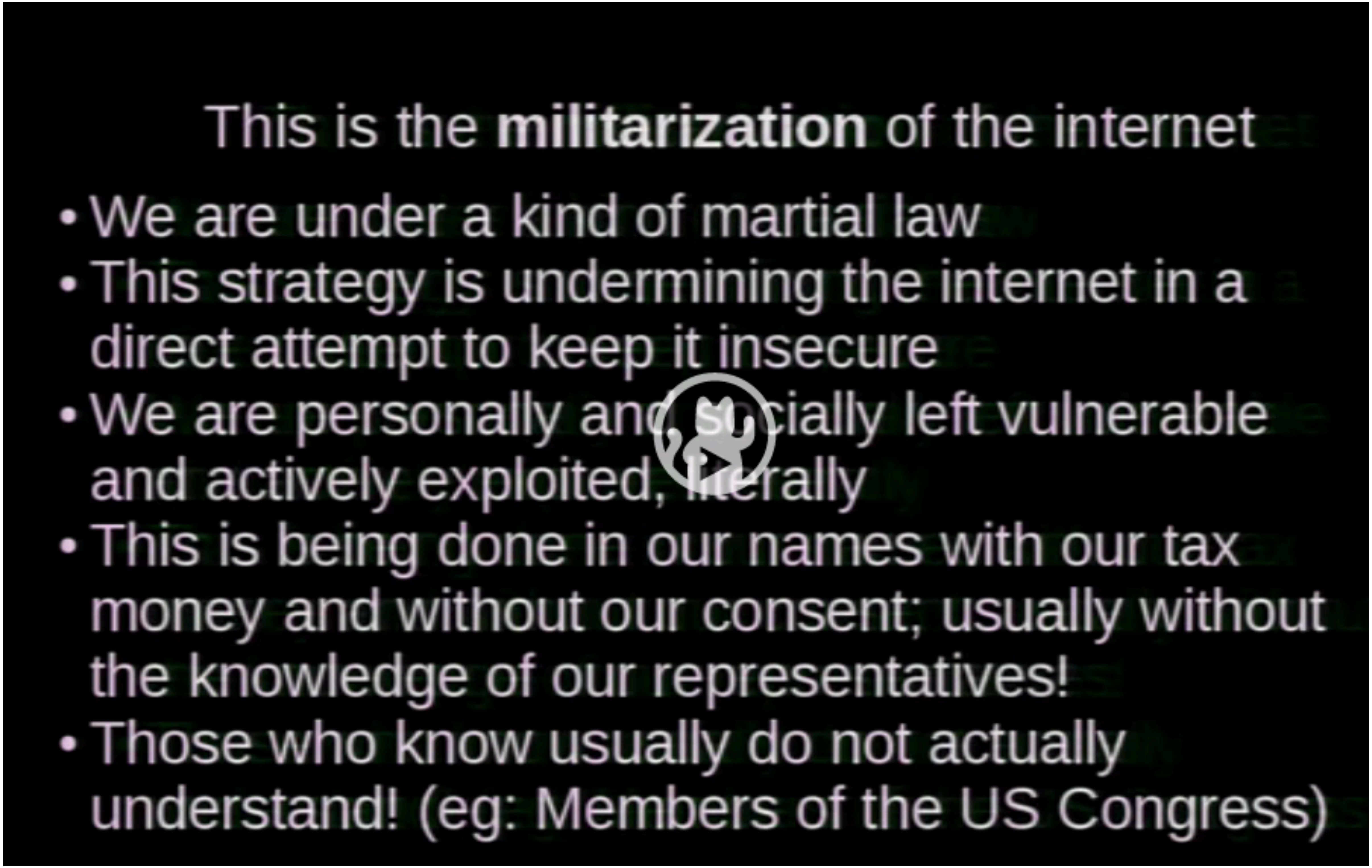
HA!

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The board generates a square wave operating at a preset frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal, the illuminating signal is amplitude-modulated (AM) with the square wave. This signal is re-radiated, where it is picked up by the radar, then processed to

2013

30C3



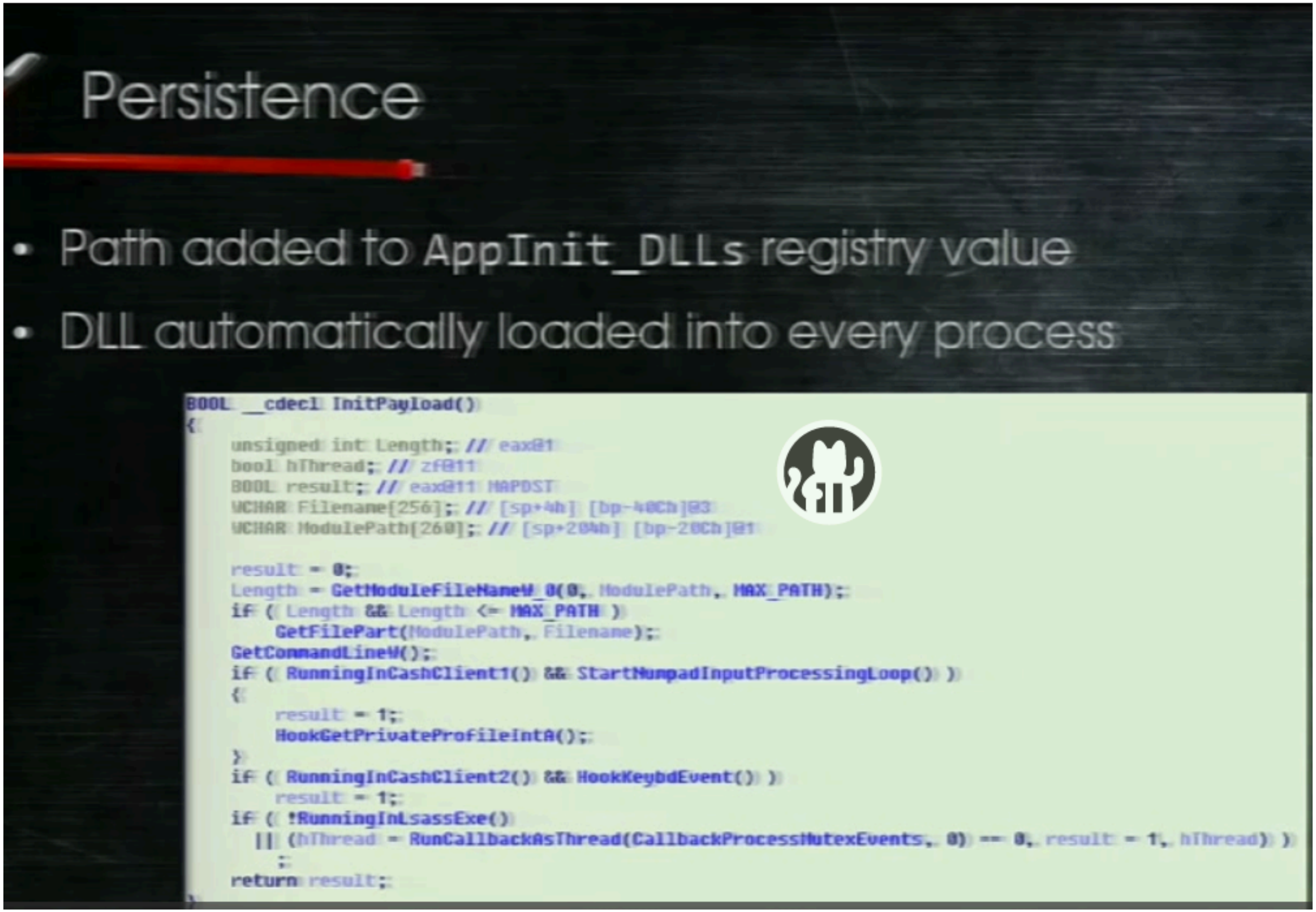
This is the **militarization** of the internet

- We are under a kind of martial law
- This strategy is undermining the internet in a direct attempt to keep it insecure
- We are personally and socially left vulnerable and actively exploited, literally
- This is being done in our names with our tax money and without our consent; usually without the knowledge of our representatives!
- Those who know usually do not actually understand! (eg: Members of the US Congress)

Electronic Bank Robberies

Stealing Money from ATMs with Malware

tw and sb



Persistence

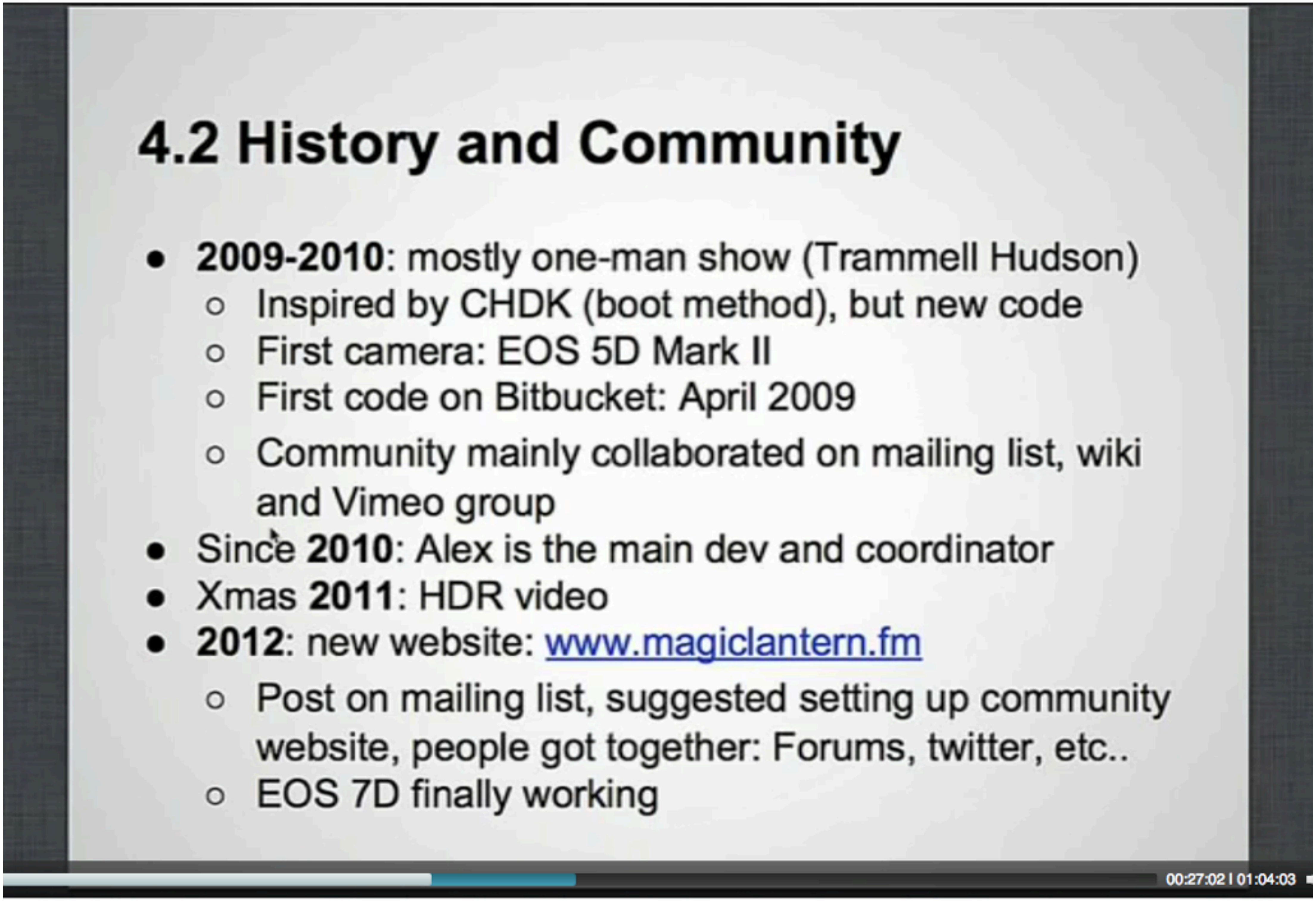
- Path added to `AppInit_DLLs` registry value
- DLL automatically loaded into every process

```
BOOL __cdecl InitPayload()
{
    unsigned int Length; // eax@1
    bool hThread; // zf@11
    BOOL result; // eax@11 MAPDST
    WCHAR Filename[256]; // [sp+4h] [bp-40Ch]@3
    WCHAR ModulePath[260]; // [sp+204h] [bp-20Ch]@1

    result = 0;
    Length = GetModuleFileNameW_0(0, ModulePath, MAX_PATH);
    if ( Length && Length <= MAX_PATH )
        GetFilePart(ModulePath, Filename);
    GetCommandLineW();
    if ( RunningInCashClient1() && StartNumpadInputProcessingLoop() )
    {
        result = 1;
        HookGetPrivateProfileIntA();
    }
    if ( RunningInCashClient2() && HookKeybdEvent() )
        result = 1;
    if ( !RunningInLsassExe()
      || (hThread = RunCallbackAsThread(CallbackProcessMutexEvents, 0) == 0, result = 1, hThread) )
        ;
    return result;
}
```

Magic Lantern

Free Software on Your Camera

Michael Zöller

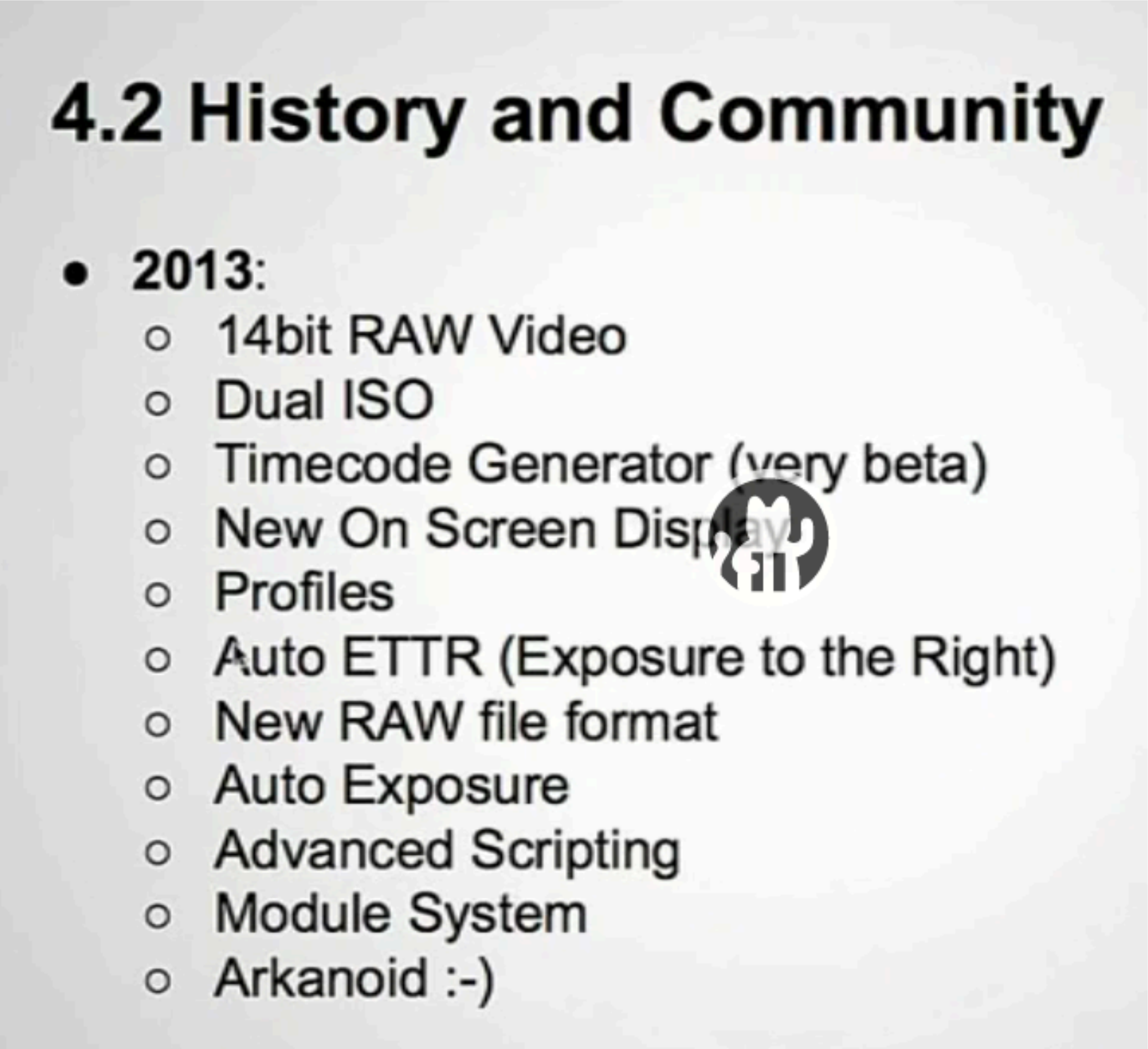


4.2 History and Community

- **2009-2010**: mostly one-man show (Trammell Hudson)
    - Inspired by CHDK (boot method), but new code
    - First camera: EOS 5D Mark II
    - First code on Bitbucket: April 2009
    - Community mainly collaborated on mailing list, wiki and Vimeo group
- Since **2010**: Alex is the main dev and coordinator
- Xmas **2011**: HDR video
- **2012**: new website: www.magiclantern.fm
    - Post on mailing list, suggested setting up community website, people got together: Forums, twitter, etc..
    - EOS 7D finally working

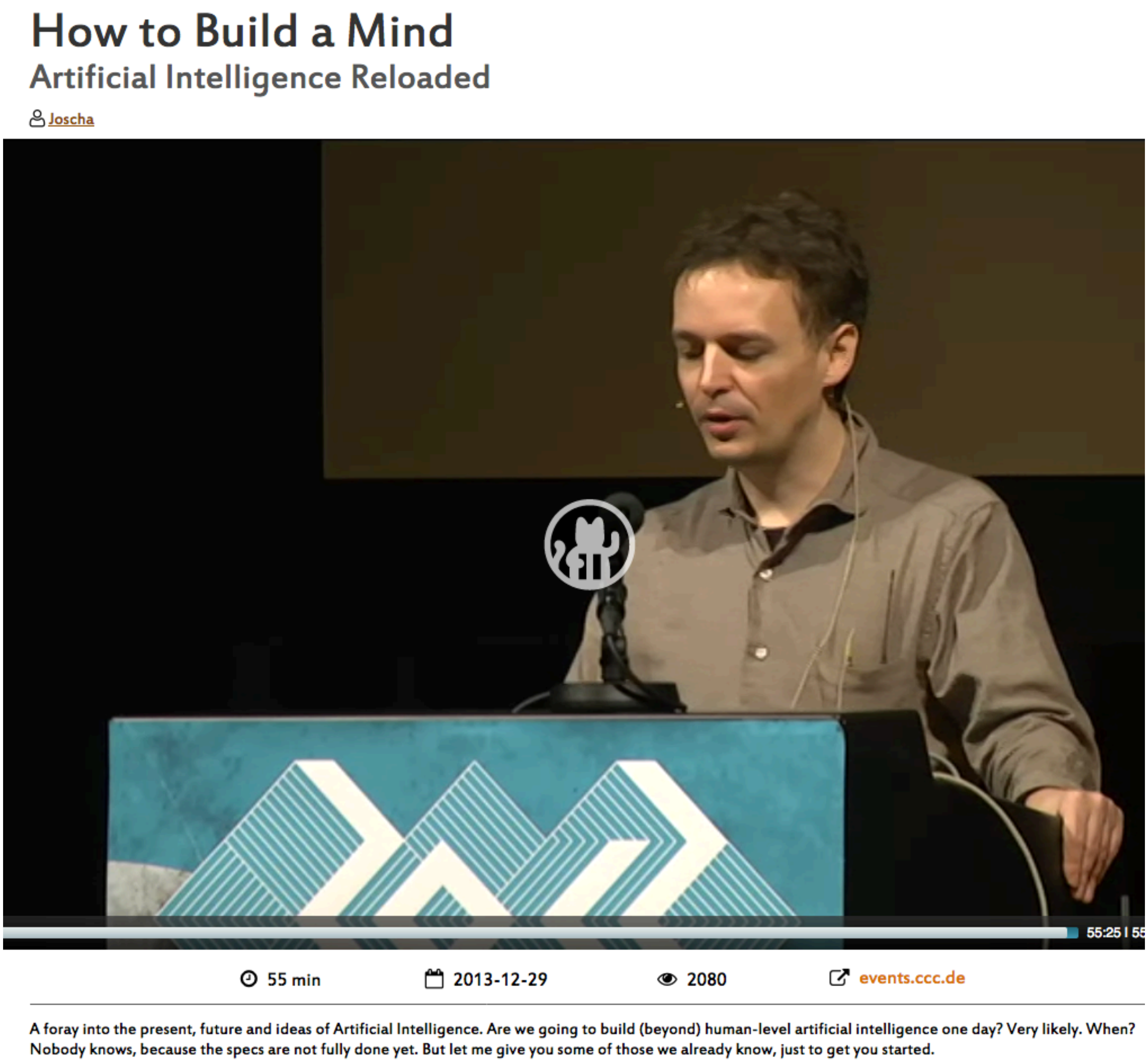
64 min | 2013-12-28 | 1057 | events.ccc.de

We present Magic Lantern, a free open software add-on for Canon DSLR cameras, that offers increased functionality aimed mainly at DSLR pro and power users. It runs alongside Canon's own firmware and introduces to consumer-grade DSLRs features usually only found in professional high-end digital (cinema) cameras.



4.2 History and Community

- **2013**:
  - 14bit RAW Video
  - Dual ISO
  - Timecode Generator (very beta)
  - New On Screen Display
  - Profiles
  - Auto ETTR (Exposure to the Right)
  - New RAW file format
  - Auto Exposure
  - Advanced Scripting
  - Module System
  - Arkanoid :-)



How to Build a Mind

Artificial Intelligence Reloaded

Joscha

55 min

2013-12-29

2080

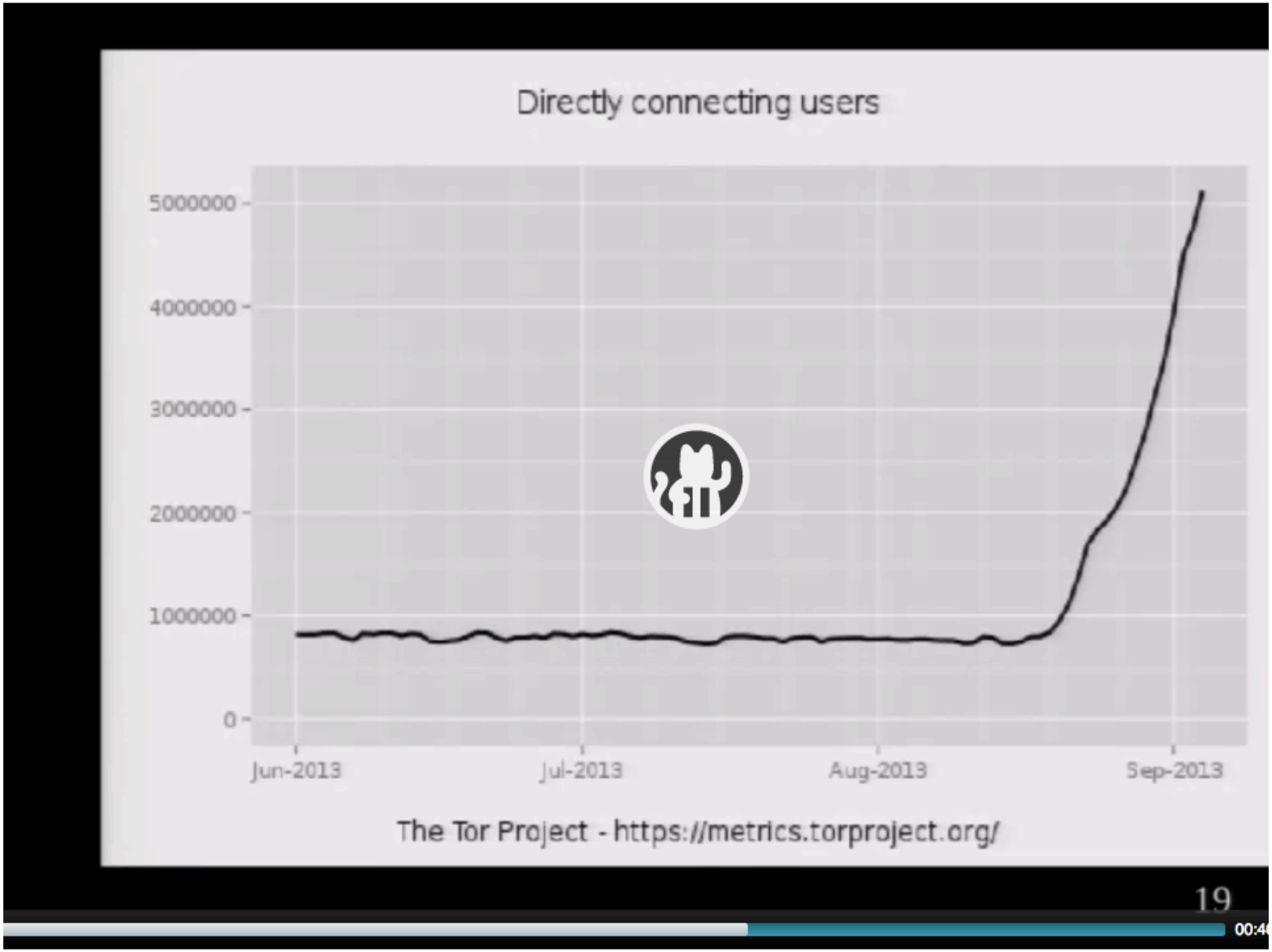
events.ccc.de

A foray into the present, future and ideas of Artificial Intelligence. Are we going to build (beyond) human-level artificial intelligence one day? Very likely. When? Nobody knows, because the specs are not fully done yet. But let me give you some of those we already know, just to get you started.

The Tor Network

We're living in interesting times

Jacob and arma



Directly connecting users

The Tor Project - https://metrics.torproject.org/

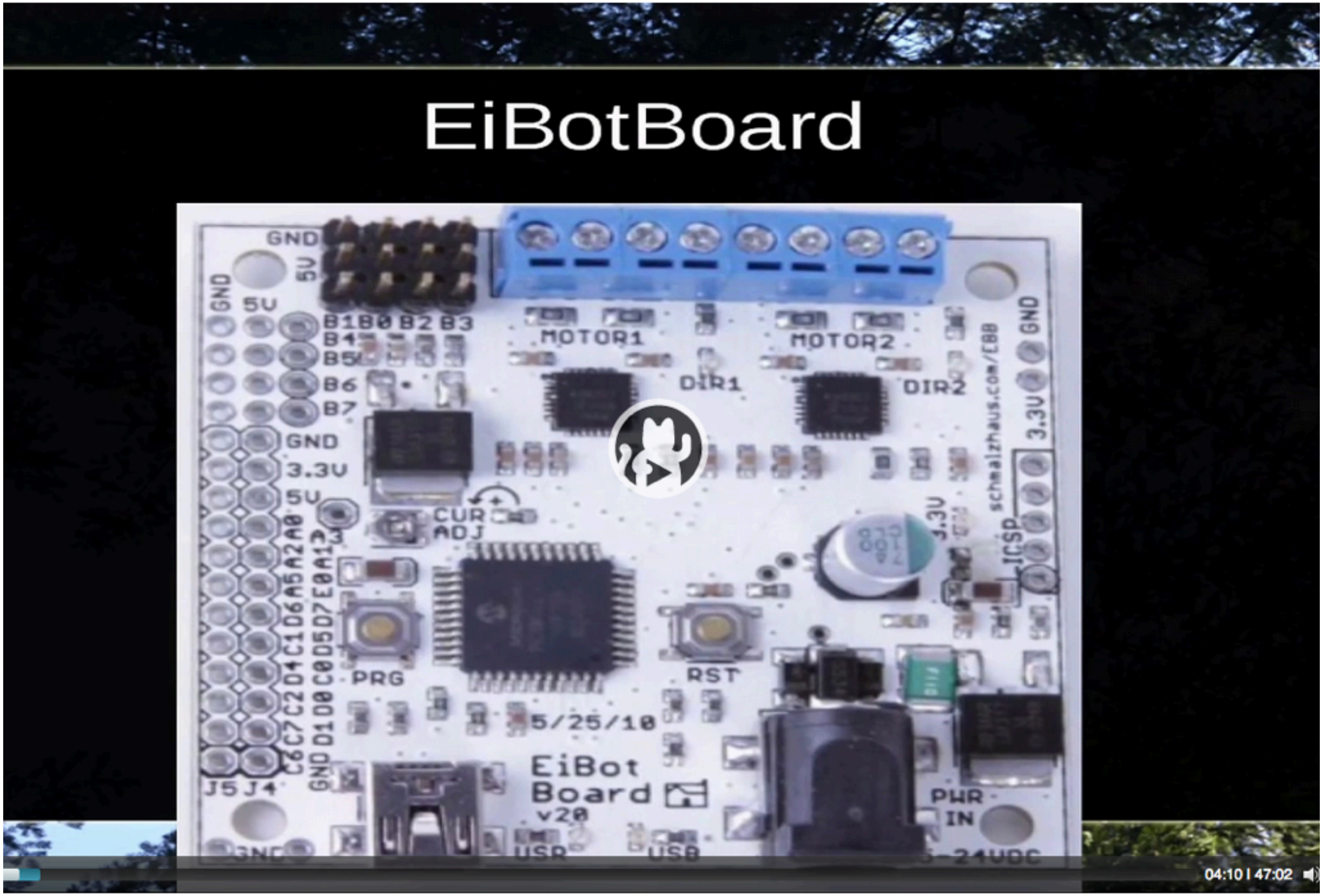
62 min 2013-12-27 2013-12-31 2078 events.ccc.de

Roger Dingledine and Jacob Appelbaum will discuss contemporary Tor Network issues related to censorship, security, privacy and anonymity online.

Hillbilly Tracking of Low Earth Orbit

Repurposing an Inmarsat Dish

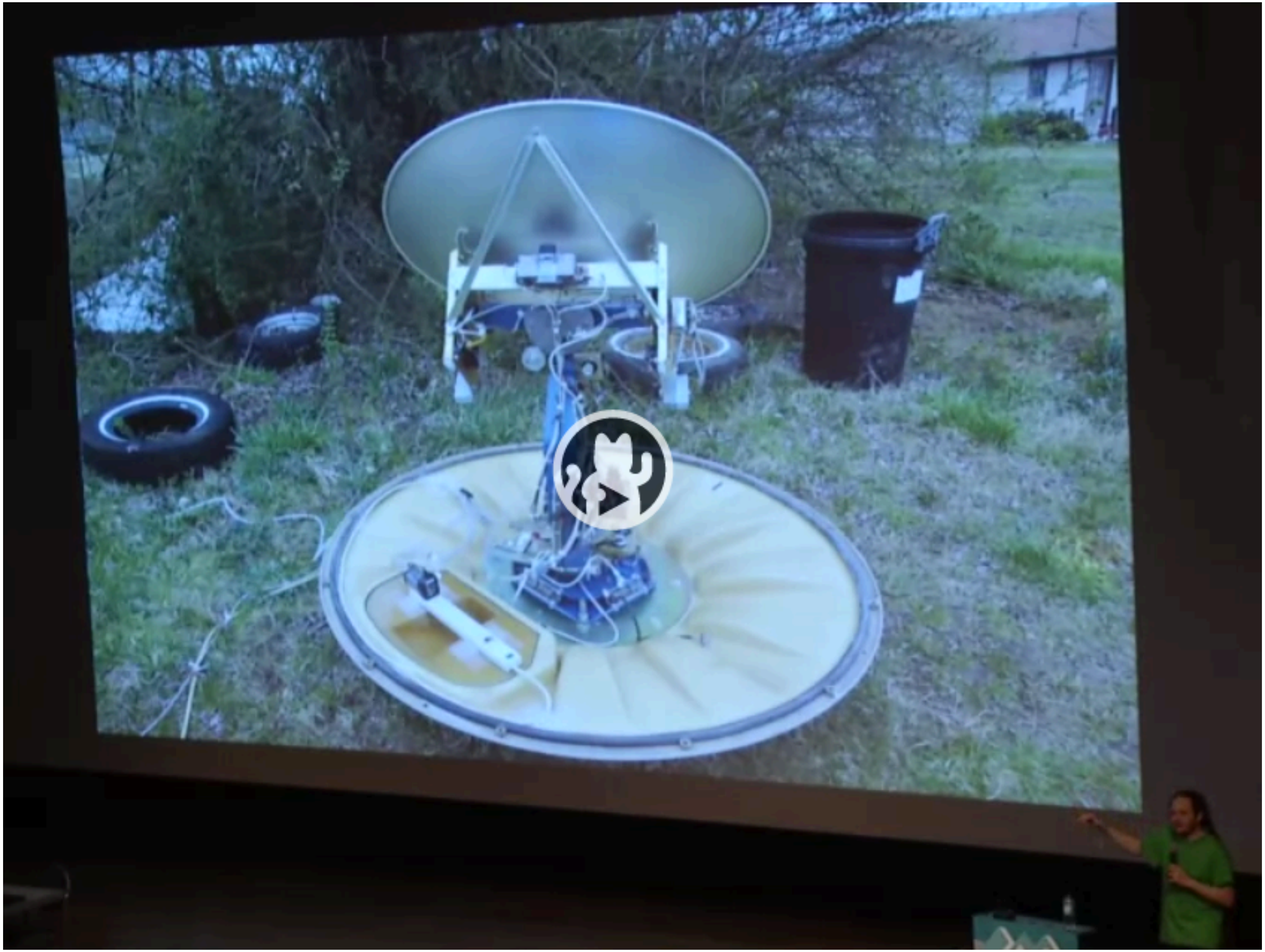
Travis Goodspeed

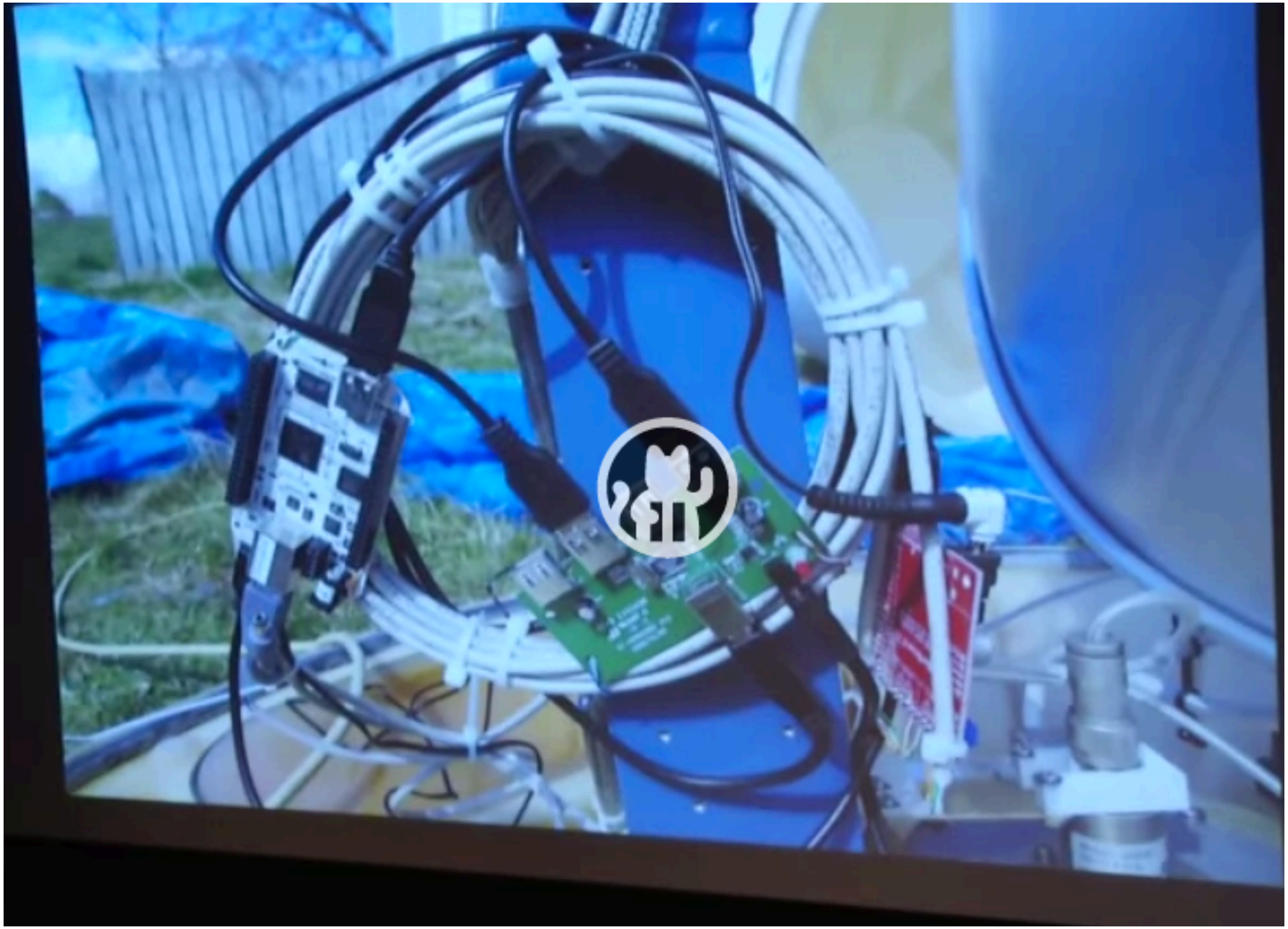


EiBotBoard

47 min 2013-12-28 2026 events.ccc.de

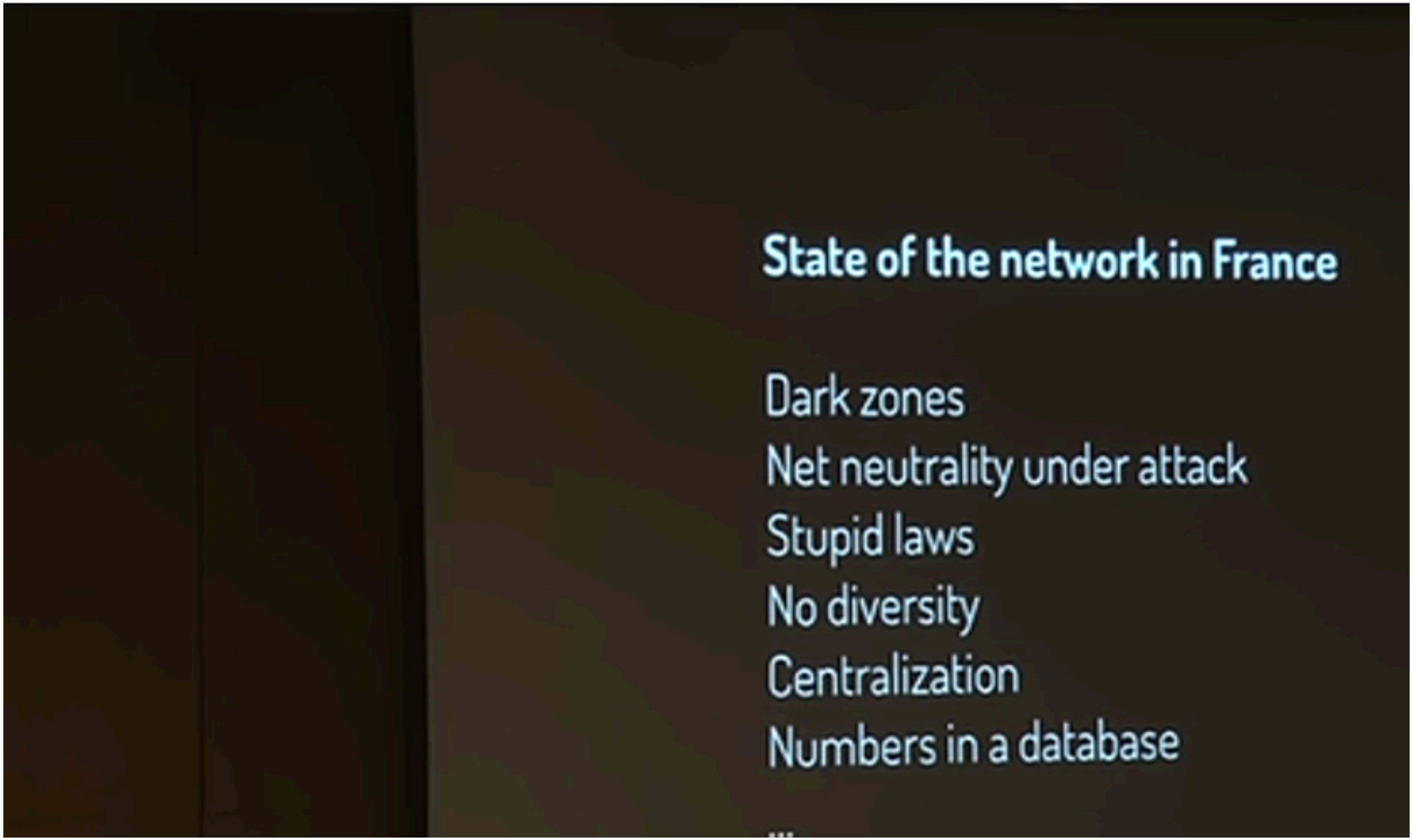
Satellites in Low Earth Orbit have tons of nifty signals, but they move quickly though the sky and are difficult to track with fine accuracy. This lecture describes a remotely operable satellite tracking system that the author built from a Navy-surplus Inmarsat dish in Southern Appalachia.





Y U NO ISP, taking back the Net

taziden



State of the network in France

Dark zones

Net neutrality under attack

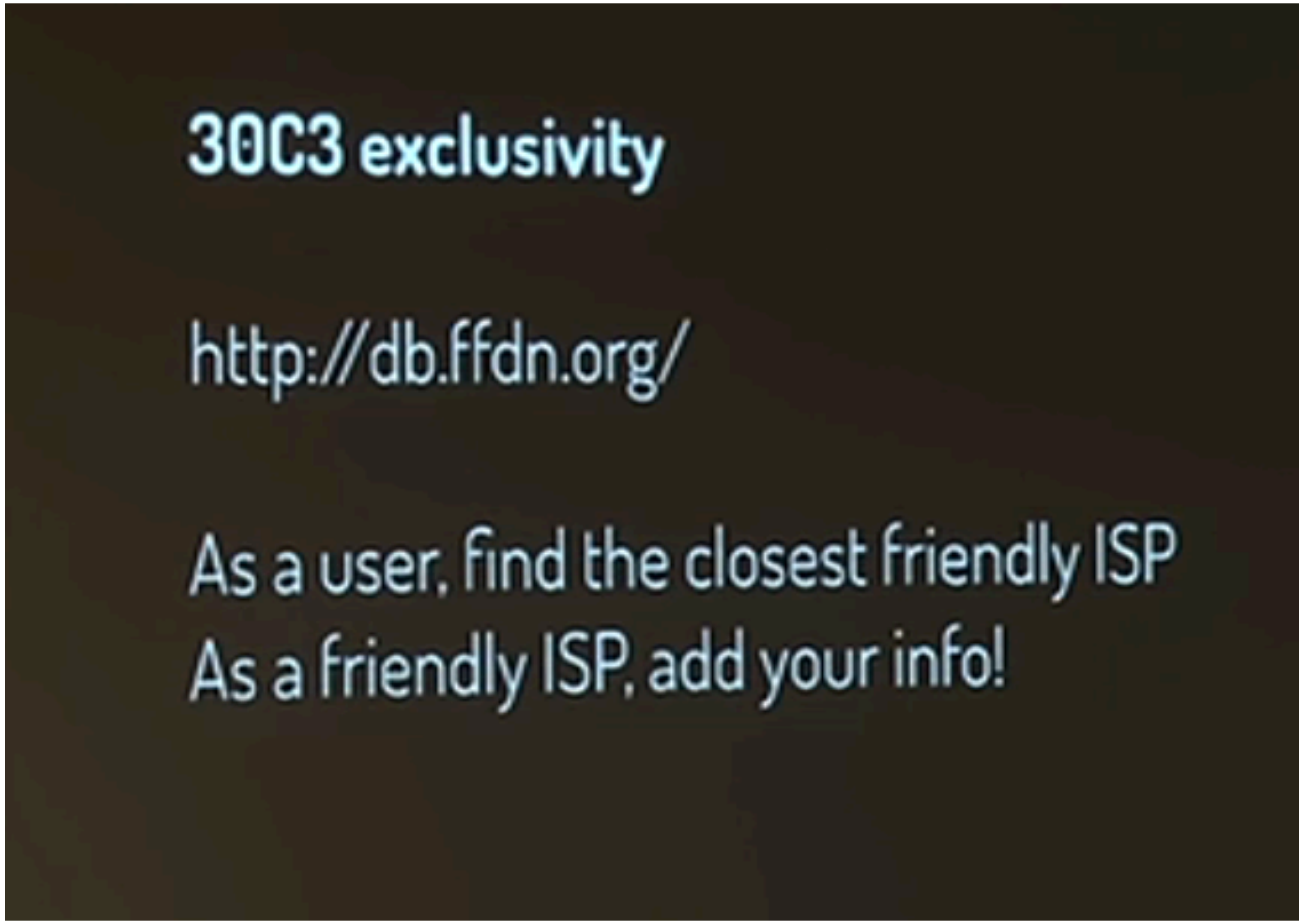
Stupid laws

No diversity

Centralization

Numbers in a database

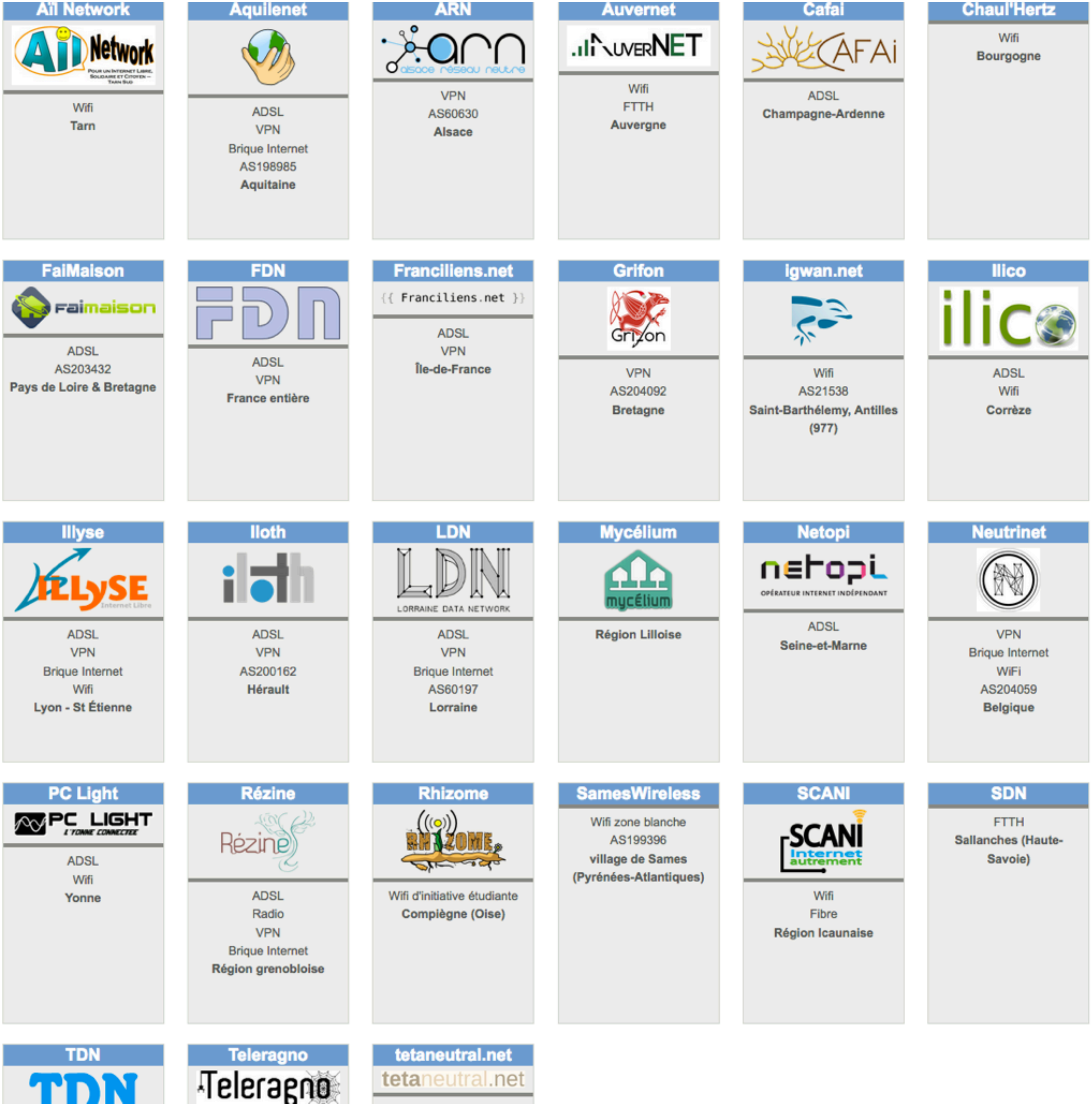
...



30C3 exclusivity

http://db.ffdn.org/

As a user, find the closest friendly ISP
As a friendly ISP, add your info!



Aïl Network

Wifi
Tarn

Aquilenet

ADSL
VPN
Brique Internet
AS198985
Aquitaine

ARN

VPN
AS60630
Alsace

Auvernet

Wifi
FTTH
Auvergne

Cafai

ADSL
Champagne-Ardenne

Chaul'Hertz

Wifi
Bourgogne

FaiMaison

ADSL
AS203432
Pays de Loire & Bretagne

FDN

ADSL
VPN
France entière

Franciliens.net

ADSL
VPN
Île-de-France

Grifon

VPN
AS204092
Bretagne

Igwan.net

Wifi
AS21538
Saint-Barthélemy, Antilles (977)

Ilico

ADSL
Wifi
Corrèze

Illyse

ADSL
VPN
Brique Internet
Wifi
Lyon - St Étienne

Iloth

ADSL
VPN
AS200162
Hérault

LDN

ADSL
VPN
Brique Internet
AS60197
Lorraine

Mycélium

Région Lilloise

Netopi

ADSL
Seine-et-Marne

Neutrinet

VPN
Brique Internet
WiFi
AS204059
Belgique

PC Light

ADSL
Wifi
Yonne

Rézine

ADSL
Radio
VPN
Brique Internet
Région grenobloise

Rhizome

Wifi d'initiative étudiante
Compiègne (Oise)

SamesWireless

Wifi zone blanche
AS199396
village de Sames (Pyrénées-Atlantiques)

SCANI

Wifi
Fibre
Région Icaunaise

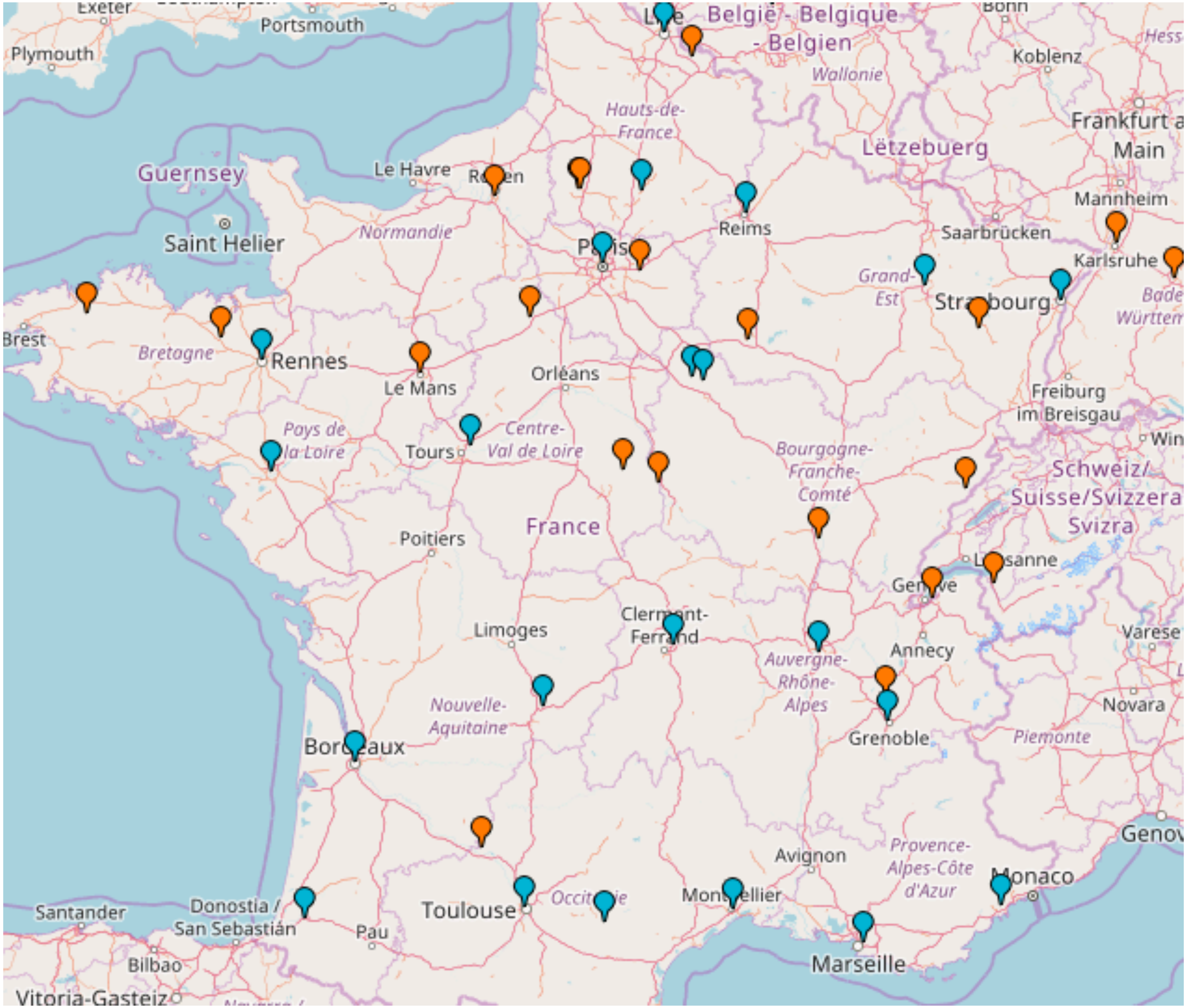
SDN

FTTH
Sallanches (Haute-Savoie)

TDN

Telearagno

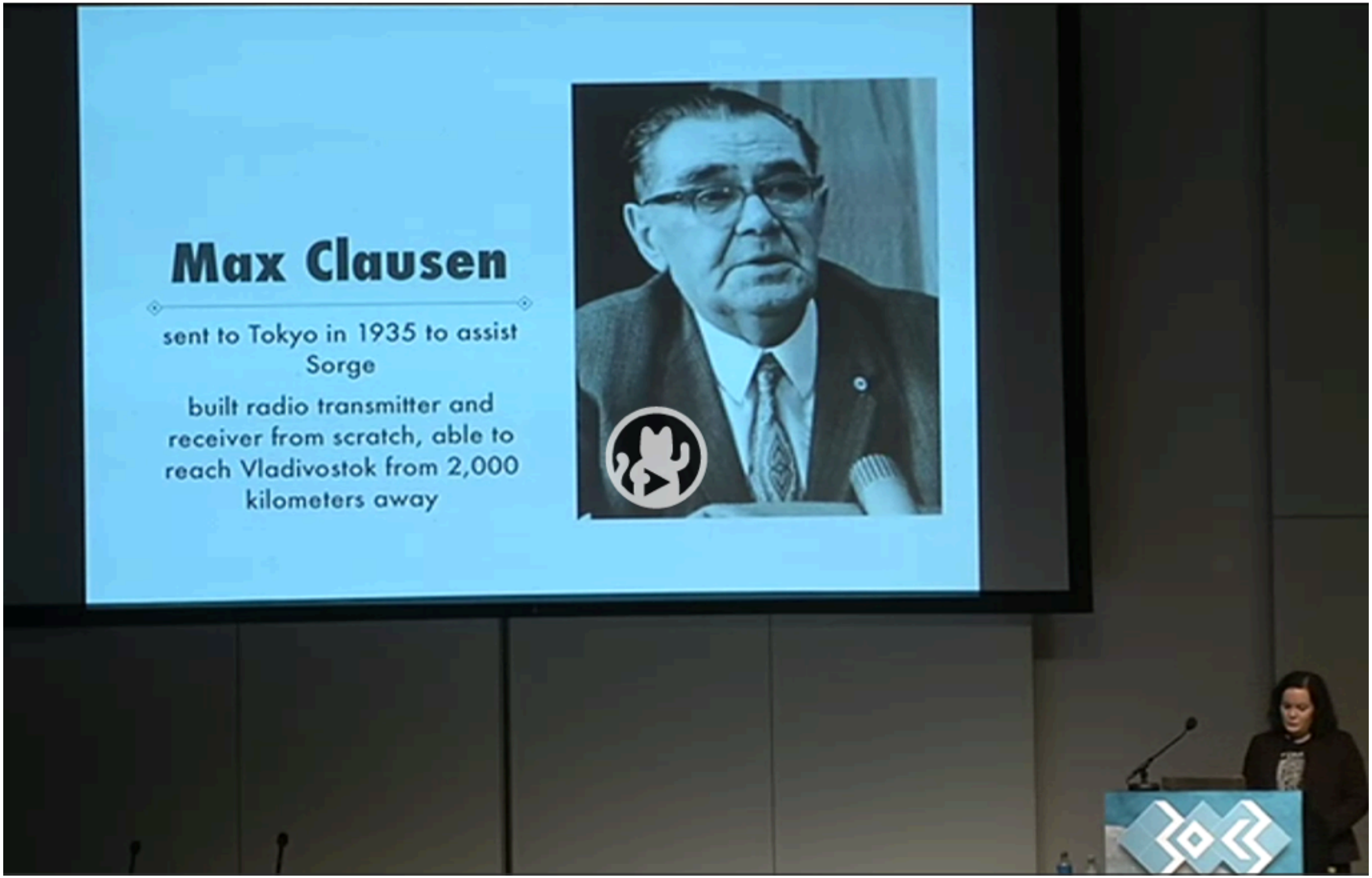
tetaneutral.net


Exeter
Portsmouth
Plymouth
Lille
België - Belgique - Belgien
Wallonie
Bonn
Koblenz
Hess
Hauts-de-France
Frankfurt a Main
Lëtzebuerg
Guernsey
Le Havre
Rouen
Mannheim
Saint Helier
Normandie
Paris
Reims
Saarbrücken
Karlsruhe
Grand-Est
Strasbourg
Bade Württem
Brest
Bretagne
Rennes
Le Mans
Orléans
Freiburg im Breisgau
Win
Pays de la Loire
Tours
Centre-Val de Loire
Bourgogne-Franche-Comté
Schweiz/Suisse/Svizzera/Svizra
Poitiers
France
Lausanne
Genève
Clermont-Ferrand
Limoges
Varese
Annecy
Auvergne-Rhône-Alpes
Nouvelle-Aquitaine
Novara
Bordeaux
Grenoble
Piemonte
Genov
Provence-Alpes-Côte d'Azur
Avignon
Monaco
Santander
Donostia / San Sebastián
Toulouse
Occitanie
Montpellier
Pau
Bilbao
Marseille
Vitoria-Gasteiz
Navarra /

World War II Hackers

Stalin's best men, armed with paper and pen

Anja Drephal



Max Clausen

sent to Tokyo in 1935 to assist Sorge

built radio transmitter and receiver from scratch, able to reach Vladivostok from 2,000 kilometers away

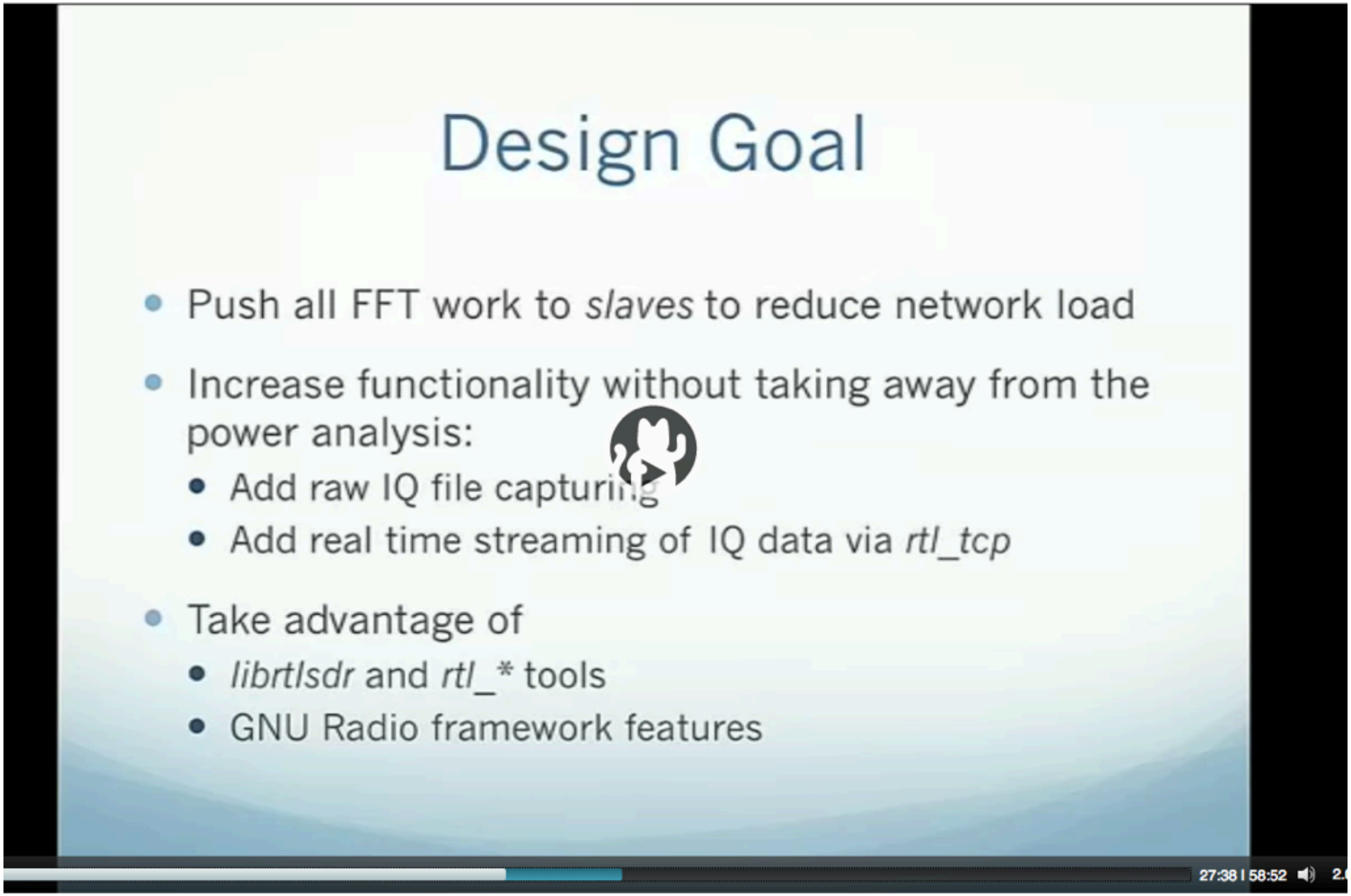
No Neutral Ground in a Burning World

Quinn Norton and Eleanor Saitta

Geeks didn't change, we just live in an eternal September now.

Monitoring the Spectrum: Building Your Own Distributed RF Scanner Array

Andrew Reiter (arr,awr)



Design Goal

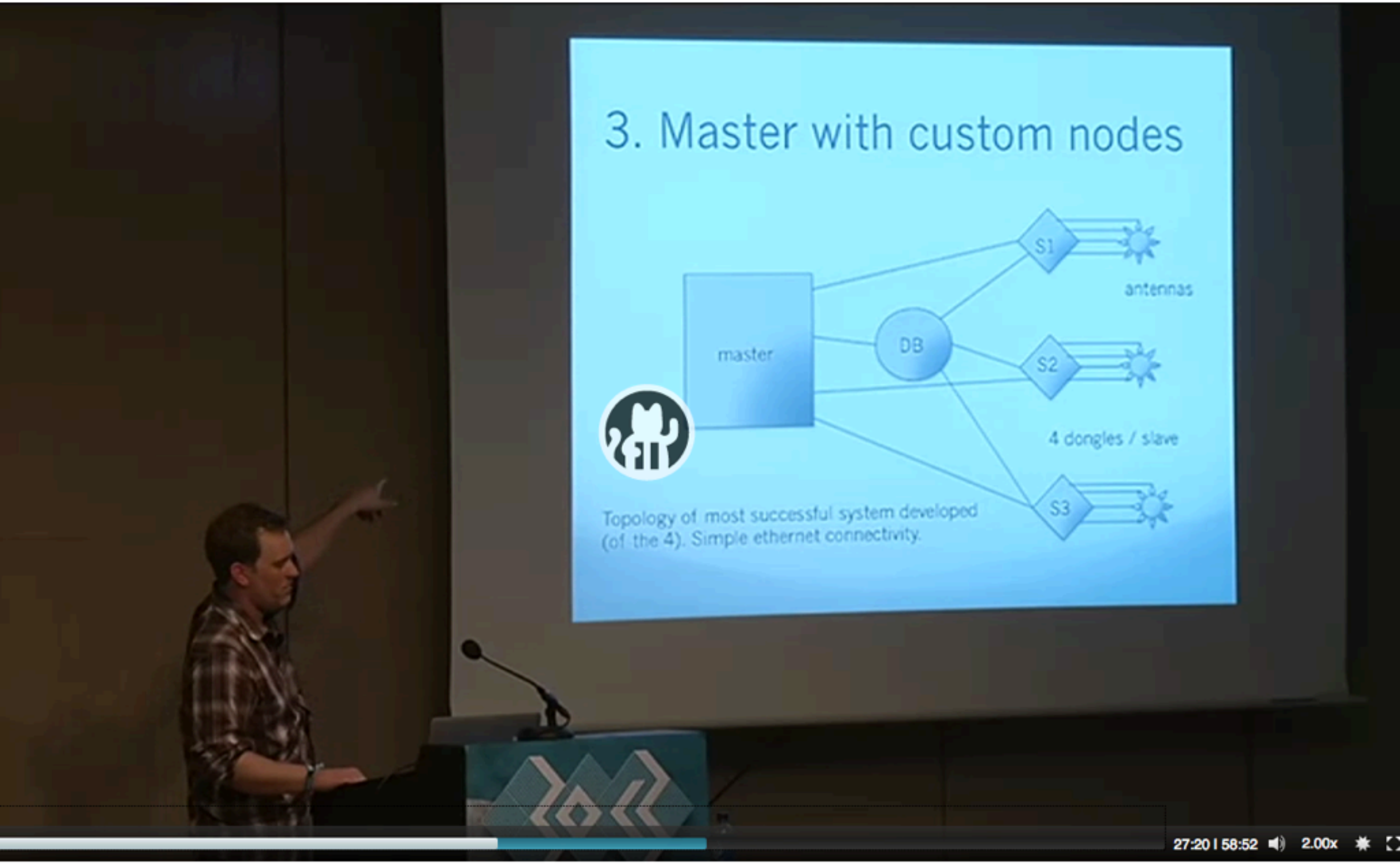
- Push all FFT work to *slaves* to reduce network load
- Increase functionality without taking away from the power analysis:
  - Add raw IQ file capturing
  - Add real time streaming of IQ data via *rtl_tcp*
- Take advantage of
  - *librtlsdr* and *rtl_** tools
  - GNU Radio framework features

58 min 2013-12-27 2013-12-28 579 events.ccc.de

Software-Defined Radio (SDR) has increased in popularity in recent years due to the decrease in hardware costs and increase in processing power. One example of such a class of devices is the RTL-SDR USB dongles based on the Realtek RTL2832U demodulator. This talk will discuss my experience in building a distributed RF scanner array for monitoring and spectrum mapping using such cheap SDR devices. The goal is to help the audience understand the what, why, and how of building their own RF monitoring array so that they will be able to do it themselves. In this era of increasingly being "watched", we must be prepared to do our own "watching".

uted RF Scanner Array

Andrew Reiter (arr,awr)



3. Master with custom nodes

Topology of most successful system developed (of the 4). Simple ethernet connectivity.

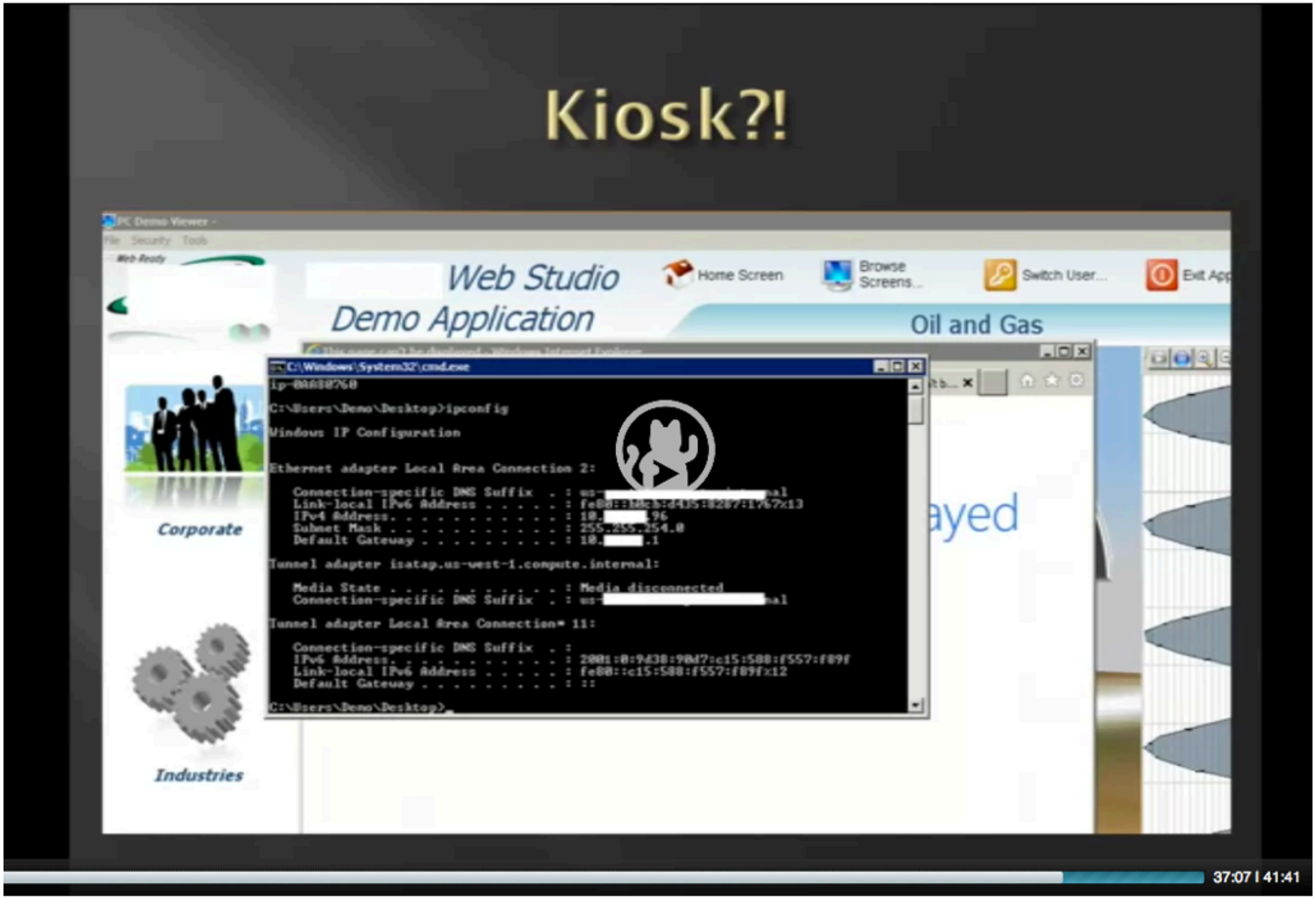
58 min 2013-12-27 2013-12-28 579 events.ccc.de

Software-Defined Radio (SDR) has increased in popularity in recent years due to the decrease in hardware costs and increase in processing power. One example of such a class of devices is the RTL-SDR USB dongles based on the Realtek RTL2832U demodulator. This talk will discuss my experience in building a distributed RF

SCADA StrangeLove 2

We already know

repdet and sgordey



Kiosk?!

C:\Windows\System32\cmd.exe

```
ip-0AA80760

C:\Users\Demo\Desktop>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : us-[redacted]al
   Link-local IPv6 Address . . . . . : fe80::18cb:d435:8287:1767%13
   IPv4 Address. . . . . . . . . . . : 10.[redacted].96
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.[redacted].1

Tunnel adapter isatap.us-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : us-[redacted]al

Tunnel adapter Local Area Connection* 11:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:9d38:90d7:c15:588:f557:f09f
   Link-local IPv6 Address . . . . . : fe80::c15:588:f557:f09f%12
   Default Gateway . . . . . . . . . : ::

C:\Users\Demo\Desktop>_
```

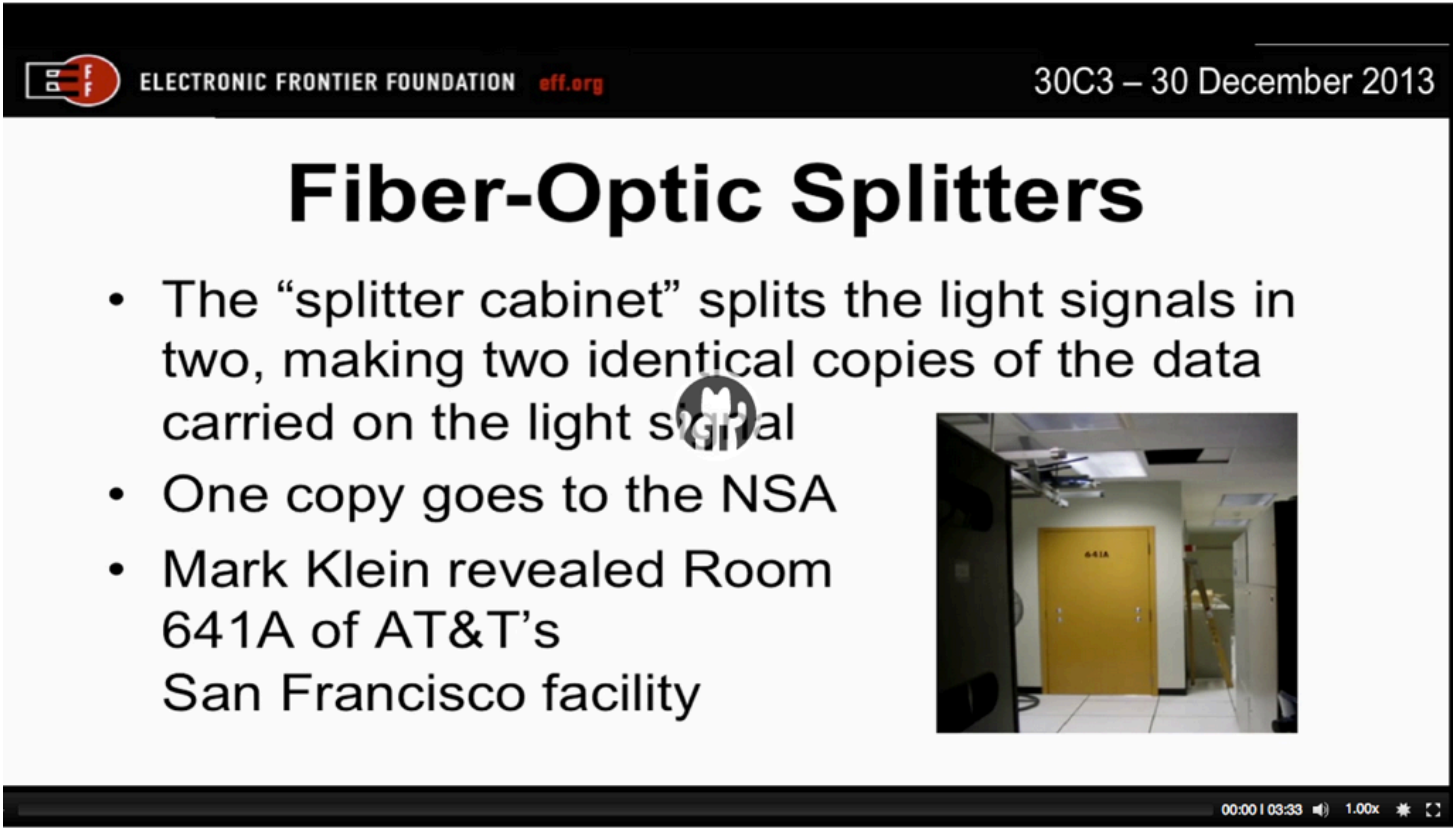
41 min 2013-12-28 436 events.ccc.de

SCADA StrangeLove team will present their research on ICS systems for the second time on CCC. Last year we showed current situation with security of industrial world and disclosed a big number of vulnerabilities found in Siemens ICS solutions. Part of vulnerabilities, we can say most notable one, wasn't disclosed due to Responsible Disclosure. This time we already know. We will speak about several industrial protocols and their weaknesses. During this year we played with new industrial hardware and software – this patitially brings new "We don't know yet" vulnerability details. Moreover, we'll mention creepiest bugs undisclosed from last year, tell you about new ones and build attack vectors from them. At last, we will share our experience in pentesting ICS enviroments.

Through a PRISM, Darkly

Everything we know about NSA spying

Kurt Opsahl



ELECTRONIC FRONTIER FOUNDATION eff.org

30C3 – 30 December 2013

Fiber-Optic Splitters

- The "splitter cabinet" splits the light signals in two, making two identical copies of the data carried on the light signal
- One copy goes to the NSA
- Mark Klein revealed Room 641A of AT&T's San Francisco facility

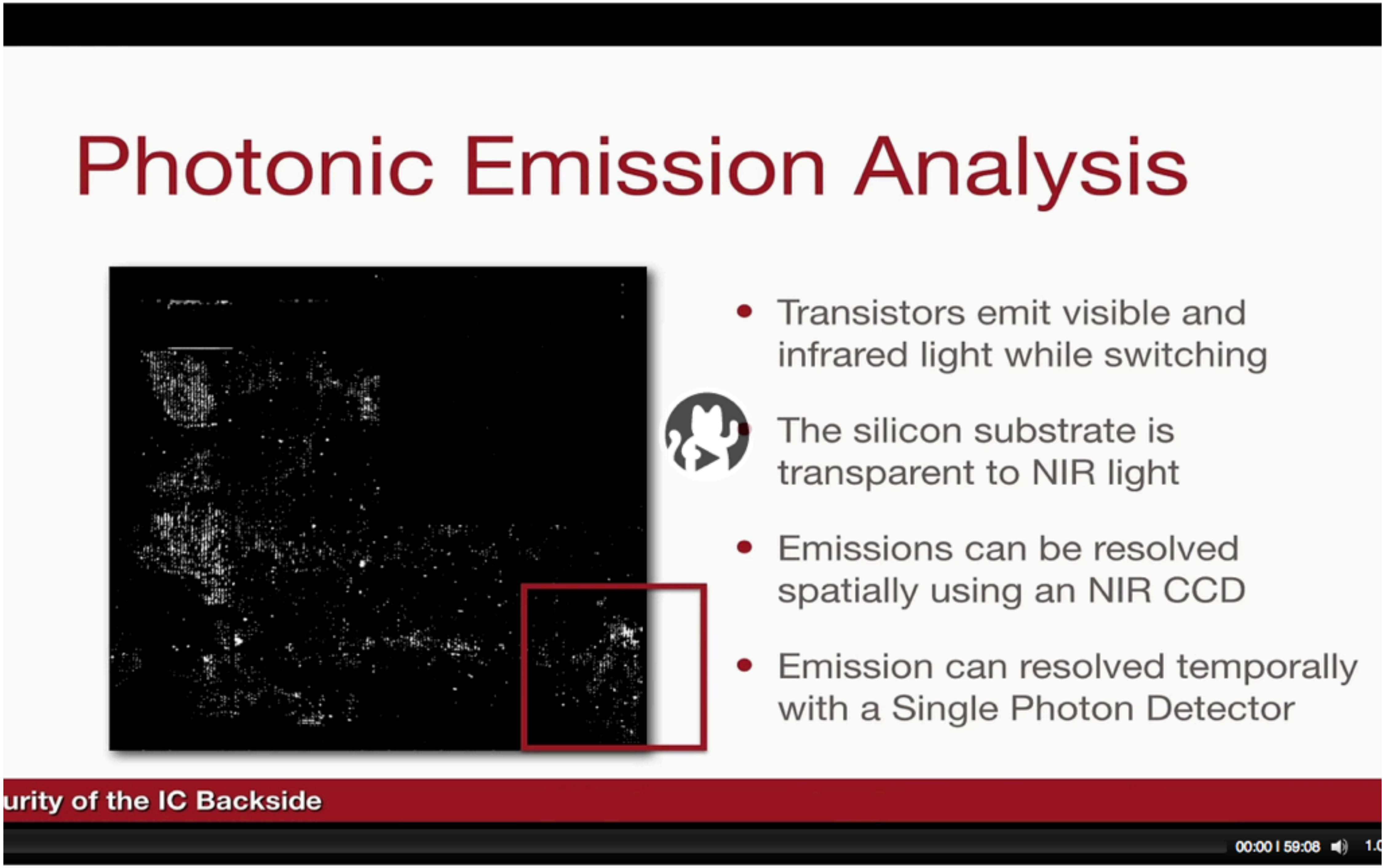
63 min | 2013-12-30 | 2013-12-31 | 421 | events.ccc.de

From Stellar Wind to PRISM, Boundless Informant to EvilOlive, the NSA spying programs are shrouded in secrecy and rubber-stamped by secret opinions from a court that meets in a faraday cage. The Electronic Frontier Foundation's Kurt Opsahl explains the known facts about how the programs operate and the laws and regulations the U.S. government asserts allows the NSA to spy on you.

Security of the IC Backside

The future of IC analysis

nedos



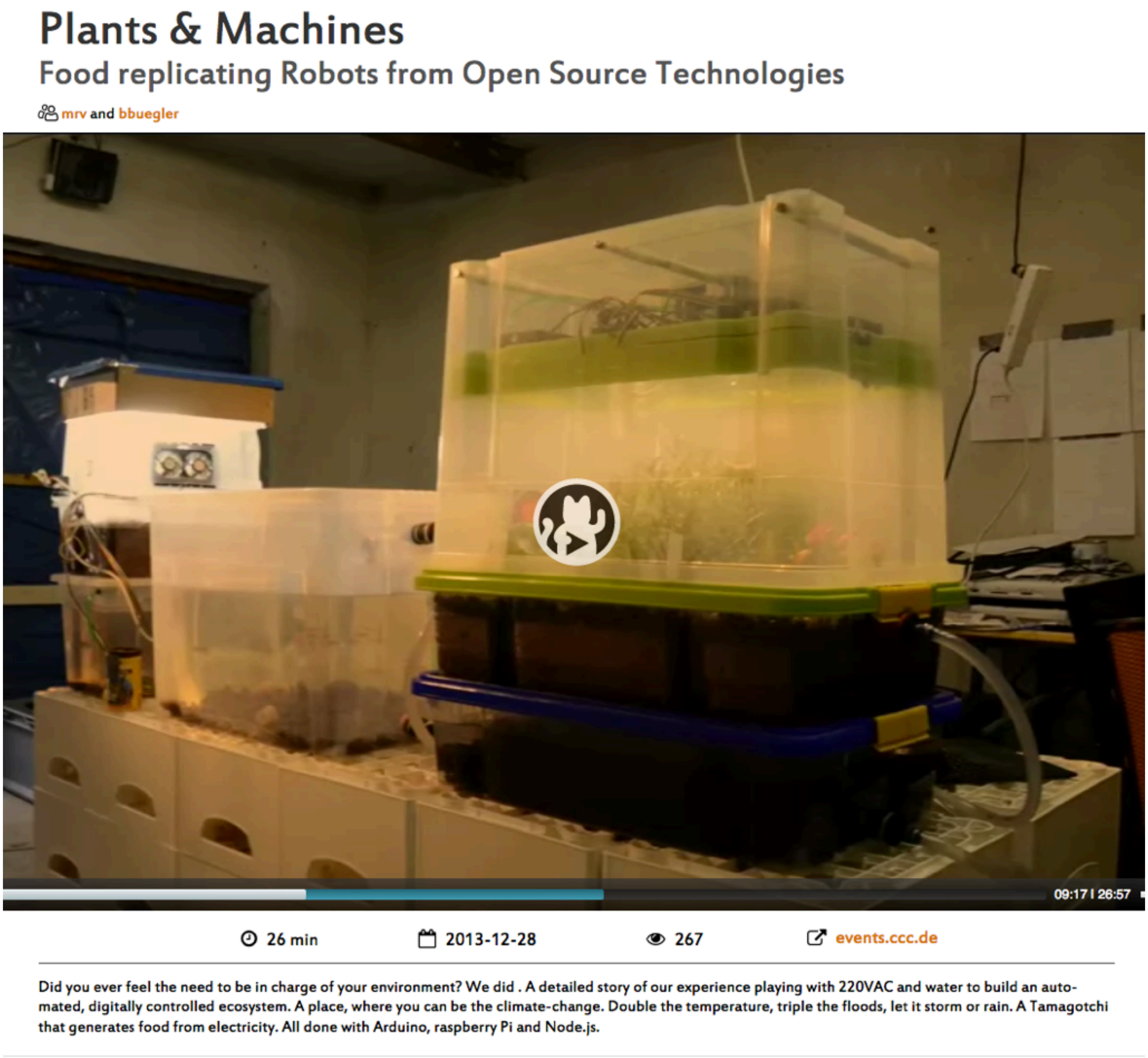
Photonic Emission Analysis

- Transistors emit visible and infrared light while switching
- The silicon substrate is transparent to NIR light
- Emissions can be resolved spatially using an NIR CCD
- Emission can resolved temporally with a Single Photon Detector

urity of the IC Backside

59 min | 2013-12-28 | 2014-01-01 | 418 | events.ccc.de

In the chain of trust of most secure schemes is an electronic chip that holds secret information. These schemes often employ cryptographically secure protocols. The weakest link of such a scheme is the chip itself. By attacking the chip directly an attacker can gain access to the secret data in its unencrypted form. In this presentation we demonstrate the attack class of the future, backside attacks. This class of attacks mitigate all device countermeasures and can access all signals of the device. As opposed to the attacks of today, these attacks can also be applied to complex systems such as the ARM SoCs of modern smartphones.



Plants & Machines

Food replicating Robots from Open Source Technologies

mrv and bbuegler

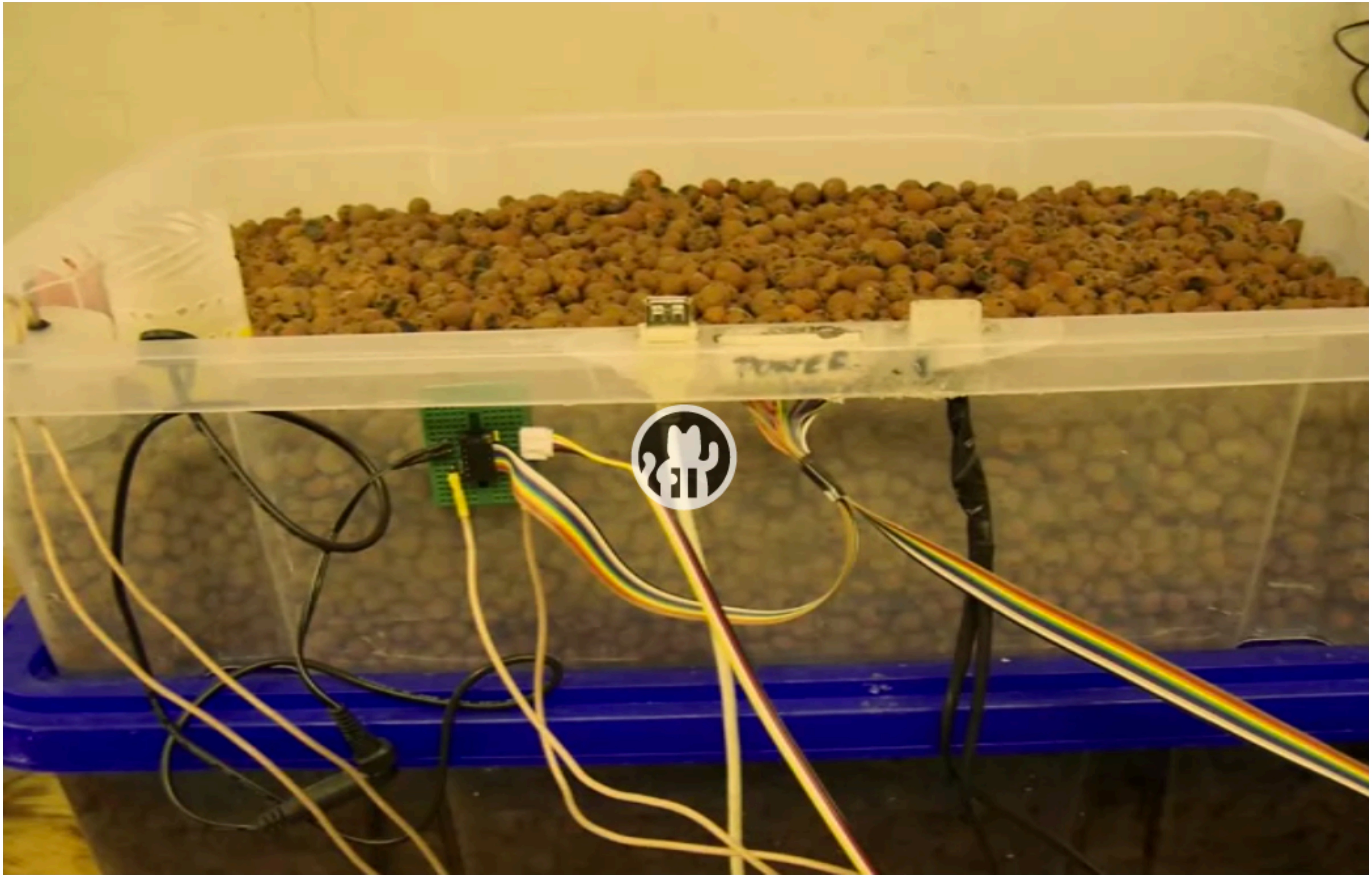
26 min

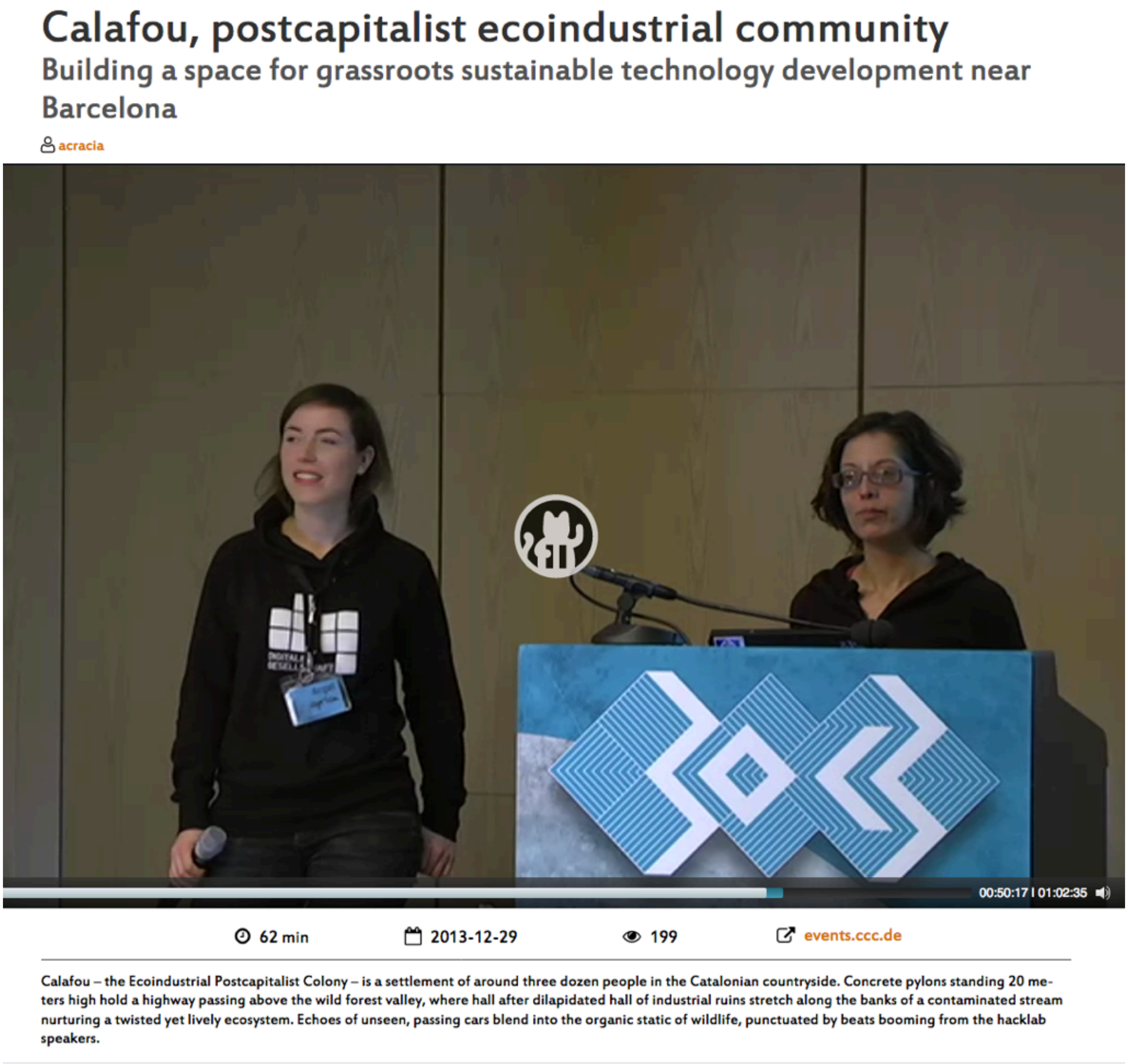
2013-12-28

👁 267

events.ccc.de

Did you ever feel the need to be in charge of your environment? We did . A detailed story of our experience playing with 220VAC and water to build an automated, digitally controlled ecosystem. A place, where you can be the climate-change. Double the temperature, triple the floods, let it storm or rain. A Tamagotchi that generates food from electricity. All done with Arduino, raspberry Pi and Node.js.


POWER



Calafou, postcapitalist ecoindustrial community

Building a space for grassroots sustainable technology development near Barcelona

acracia

62 min 2013-12-29 199 events.ccc.de

Calafou – the Ecoindustrial Postcapitalist Colony – is a settlement of around three dozen people in the Catalonian countryside. Concrete pylons standing 20 meters high hold a highway passing above the wild forest valley, where hall after dilapidated hall of industrial ruins stretch along the banks of a contaminated stream nurturing a twisted yet lively ecosystem. Echoes of unseen, passing cars blend into the organic static of wildlife, punctuated by beats booming from the hacklab speakers.

ressources :

Blog des événements actuels du CCC:	https://events.ccc.de
Site des congrès:	https://events.ccc.de/congress/2012/wiki/Main_Page
Vidéos des conférences:	https://media.ccc.de

NICELAB_

Nicelab, Laboratoire Ouvert de Nice, Hackerspace, depuis 2011