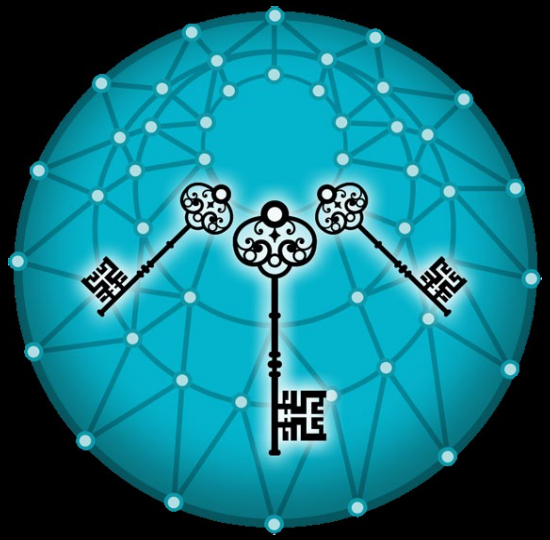
How can we protect the Internet against surveillance?



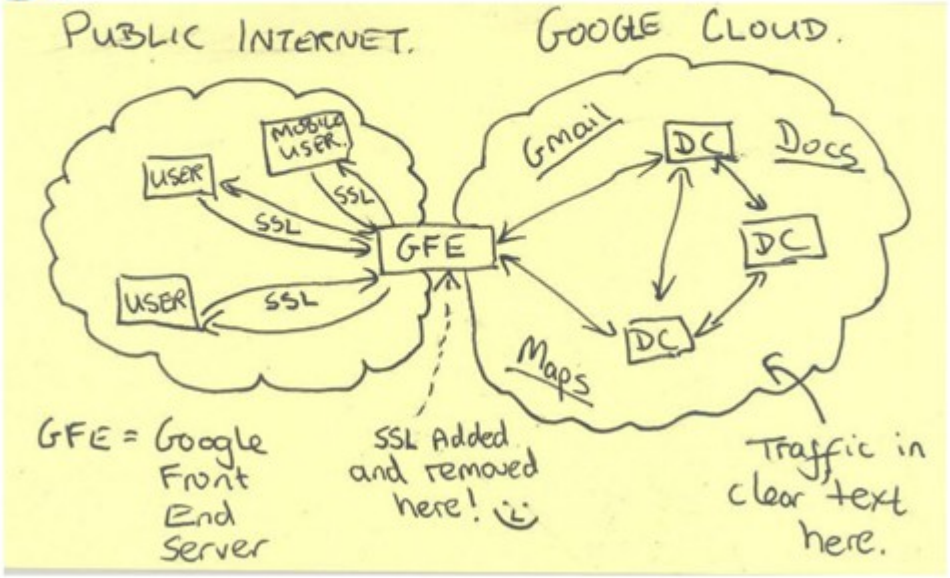
Seven TODO items for users, web developers and protocol engineers

Peter Eckersley
pde@eff.org

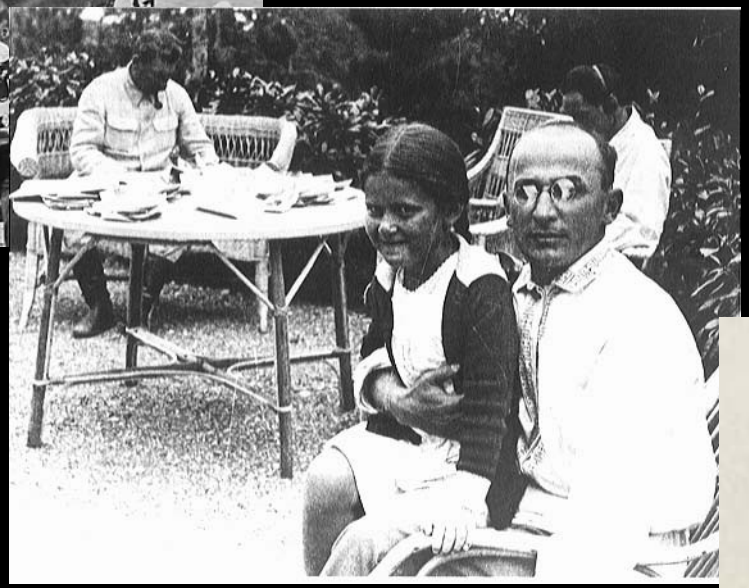
Okay, so everyone is spying on the Internet


FENDI
COACH
EST. 1941
NEW YORK
電話訪問
俄羅斯駐港領事館高值人員
我無法評論事件
俄羅斯傳媒稱
FENDI

Current Efforts - Google



It's not just the NSA...



Lots of governments are in this game!

Not to mention the commerical malware industry

These guys are fearsome, octopus-like adversaries

Does this mean we should just give up?

No.

Reason 1:

some people can't afford to give up

Reason 2:

there *is* a line we can hold

vs.

So, how do we get there?

TODO #1

Users should maximise their own security

Make sure your OS and browser are patched!

Use encryption where you can!

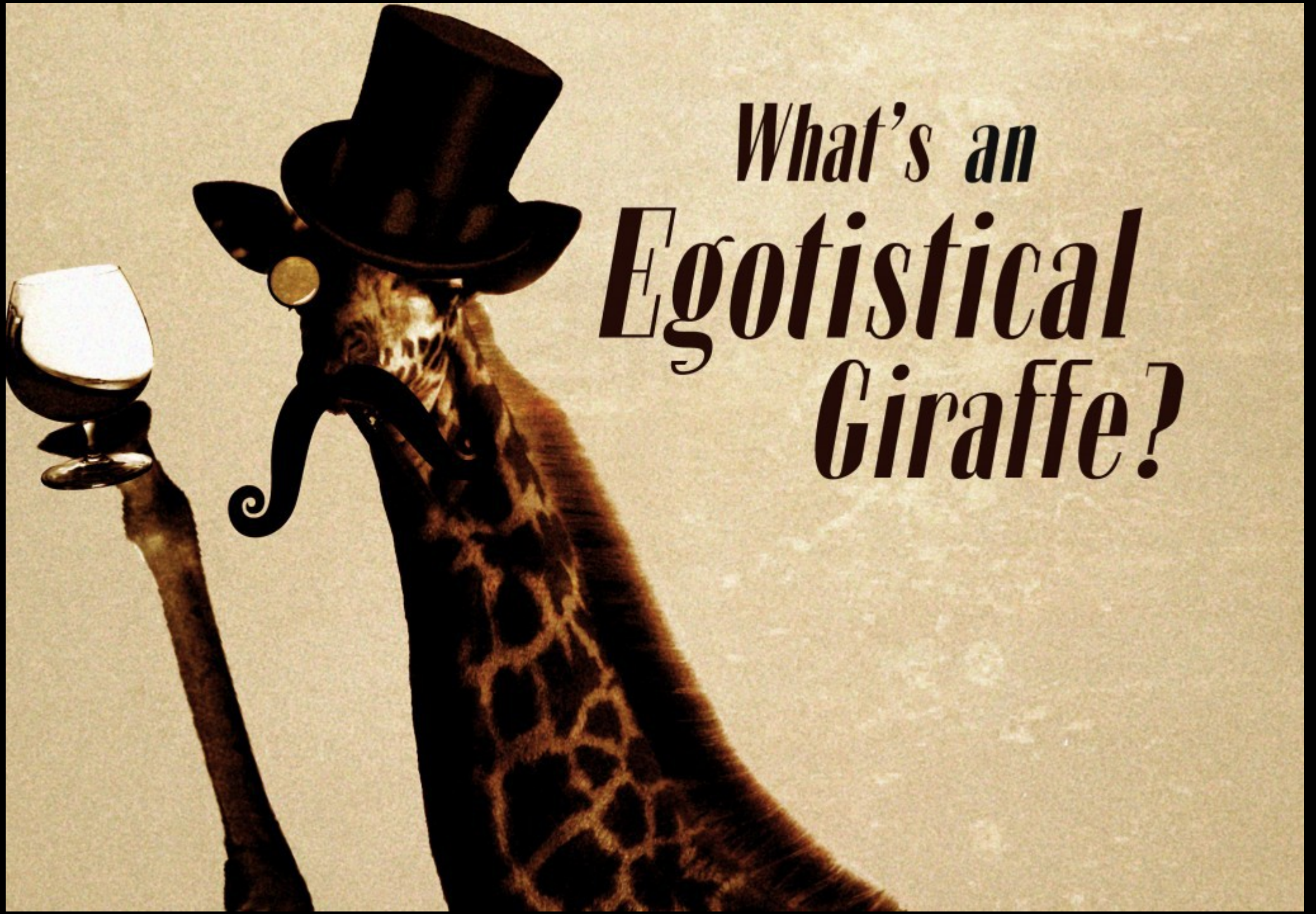
In your browser, install HTTPS Everywhere

https://eff.org/https-everywhere

For instant messaging, use OTR

(easiest with Pidgin or Adium, but be aware of the exploit risk tradeoff)

For confidential browsing,
use the Tor Browser Bundle


What's an
Egotistical
Giraffe?

Other tools to consider:

TextSecure for SMS
PGP for email (UX is terrible!)
SpiderOak etc for cloud storage
Lots of new things in the pipeline

TODO #2

Run an open wireless network!

openwireless.org

How to do this securely right now?

Chain your WPA2 network on a router below your open one.

TODO #3

Site operators...

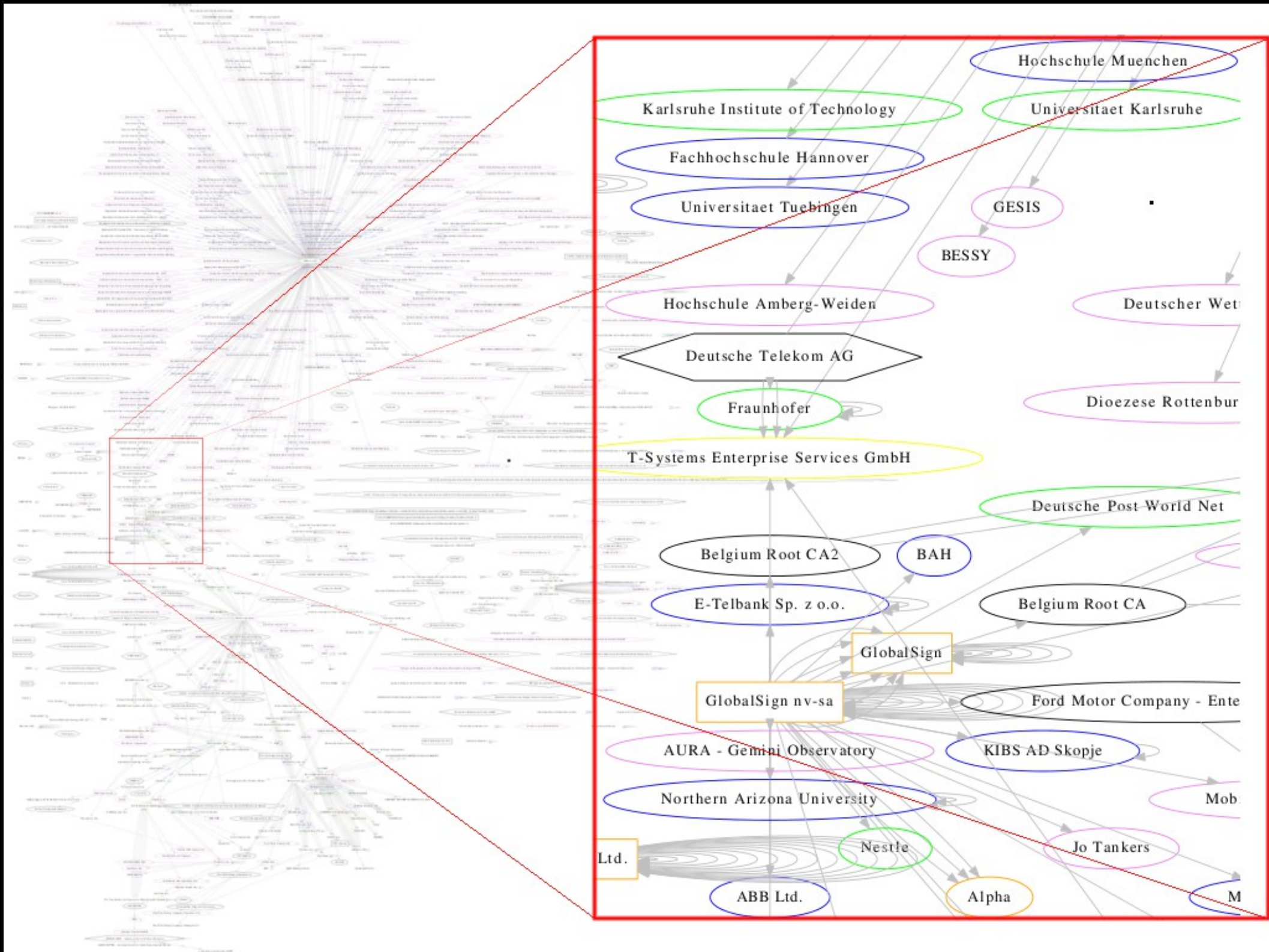
Deploy SSL/TLS/HTTPS

DEPLOY IT CORRECTLY!

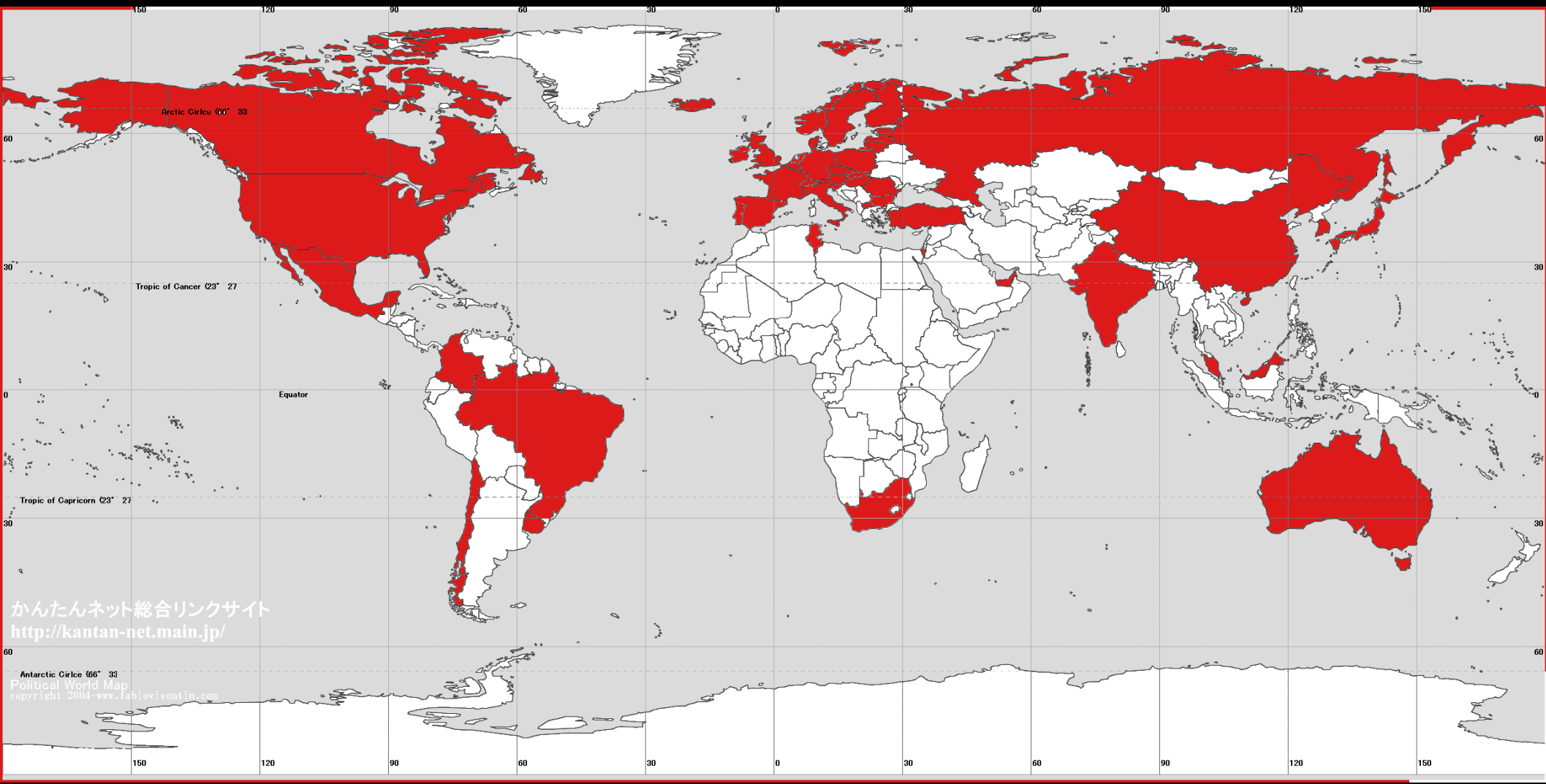
This, miserably, is a lot harder than it should be

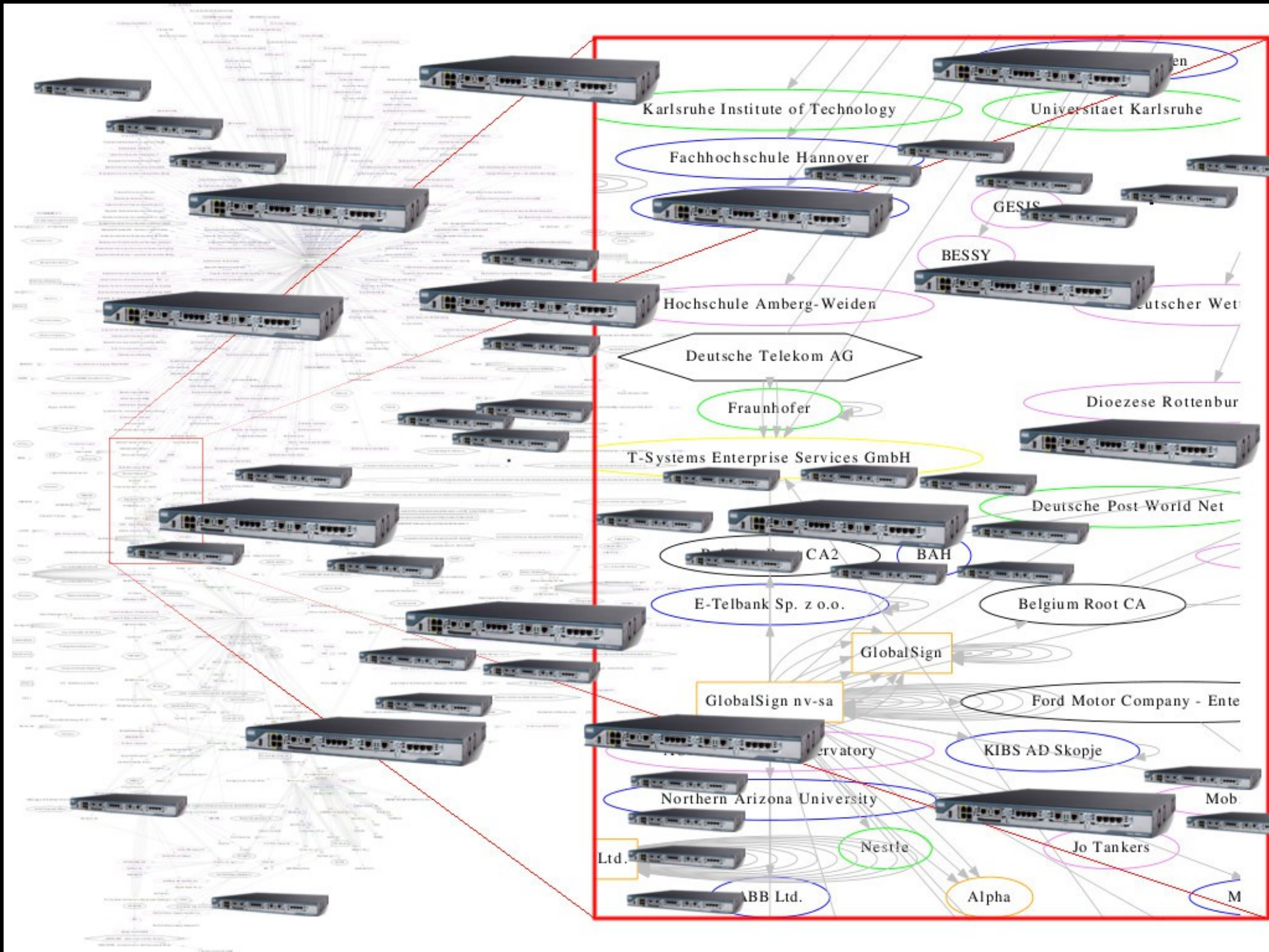
TLS/SSL Authentication


SSL
Observatory


Hochschule Muenchen
Karlsruhe Institute of Technology
Universitaet Karlsruhe
Fachhochschule Hannover
Universitaet Tuebingen
GESIS
BESSY
Hochschule Amberg-Weiden
Deutscher Wet
Deutsche Telekom AG
Dioezese Rottenbur
Fraunhofer
T-Systems Enterprise Services GmbH
Deutsche Post World Net
Belgium Root CA2
BAH
E-Telbank Sp. z o.o.
Belgium Root CA
GlobalSign
GlobalSign nv-sa
Ford Motor Company - Ente
AURA - Gemini Observatory
KIBS AD Skopje
Northern Arizona University
Mob
Nestle
Jo Tankers
Ltd.
ABB Ltd.
Alpha
M

Apparently, ~52 countries




Karlsruhe Institute of Technology
Universitaet Karlsruhe
Fachhochschule Hannover
GESIS
BESSY
Hochschule Amberg-Weiden
Deutsche Telekom AG
Fraunhofer
Dioezese Rottenbur
T-Systems Enterprise Services GmbH
Deutsche Post World Net
CA2
BAH
E-Telbank Sp. z o.o.
Belgium Root CA
GlobalSign
GlobalSign nv-sa
Ford Motor Company - Ente
KIBS AD Skopje
Northern Arizona University
Nestle
Jo Tankers
Alpha

These are usually specialist, narrowly targetted attacks

(but that's several entire other talks...

we're working on making HTTPS
more secure, easier and saner!)

In the mean time, here's what you need

A valid certificate

HTTPS by default

Secure cookies

No “mixed content”

Perfect Forward Secrecy

A well-tuned configuration

How do I make HTTPS the default?

Firefox and Chrome:
redirect, set the HSTS header

Safari and IE:
sorry, you can't (!!!)

What's a secure cookie?

Go and check your site right now...

What is “mixed content”?

HTTP stuff inside HTTPS pages

e.g. *https://www.xda-developers.com*

Other issues and bugs in your HTTPS deployment?

https://www.ssllabs.com/ssltest/

https://www.eff.org/https-everywhere/atlas/index.html

TODO #4

Encrypt your domain's email !

There are some protocols for doing this...

(STARTTLS makes SMTP → SMTPS)

How do I check if my domain does SMTPS securely?

Send emails to and from gmail

Check the headers

```
Delivered-To: peter.eckersley@gmail.com
Received: by 10.64.233.70 with SMTP id tu6csp21032iec;
        Fri, 4 Oct 2013 03:49:08 -0700 (PDT)
X-Received: by 10.68.231.71 with SMTP id te7mr683379pbc.203.1380883748409;
        Fri, 04 Oct 2013 03:49:08 -0700 (PDT)
Return-Path: <pde@mail2.eff.org>
Received: from mail2.eff.org (mail2.eff.org. [64.147.188.12])
        by mx.google.com with ESMTPS id ql10si9136286pbb.220.1969.12.31.16.00.00
        (version=TLSv1.2 cipher=RC4-SHA bits=128/128);
        Fri, 04 Oct 2013 03:49:08 -0700 (PDT)
Received-SPF: pass (google.com: domain of pde@mail2.eff.org designates 64.147.188.12 as
permitted sender) client-ip=64.147.188.12;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of pde@mail2.eff.org designates 64.147.188.12 as
permitted sender) smtp.mail=pde@mail2.eff.org;
       dkim=neutral (bad format) header.i=@eff.org
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=eff.org; s=mail2;
    h=Date:Message-Id:Subject:From:To; bh=IPPwQL5jy1JwICuwZovwNdav5VsrfM4SyXGx0WDamb0=;

b=i1yDOgrgsFVetGm5XGsDkKMMkgyXd8kMe88COZXnYAhRx+95i+I8v5sdPLETIUbadVTuAYFVv0opibSh+ZPMfk
e6ziRMI9xqOM6InFbGG/lepA3Iqf7gNf1TOUk/PmrA;
Received: ; Fri, 04 Oct 2013 03:49:07 -0700
To: peter.eckersley@gmail.com
From: "Peter Eckersley" <pde@eff.org>
Subject: Robotic out-of-office message
Message-Id: <E1VS2wV-0002zR-TC@mail2.eff.org>
Date: Fri, 04 Oct 2013 03:49:07 -0700
```

Go and do this now, or file a ticket for your ops team!

You can use a CA-signed cert
Or even just any cert

Your MTA has settings for this!

Oh did I mention?

We have a mailing list to help large sites get this right

Google for
crypto-ops

Does this prevent “man in the middle” attacks?

No. We're working on that, but remember...

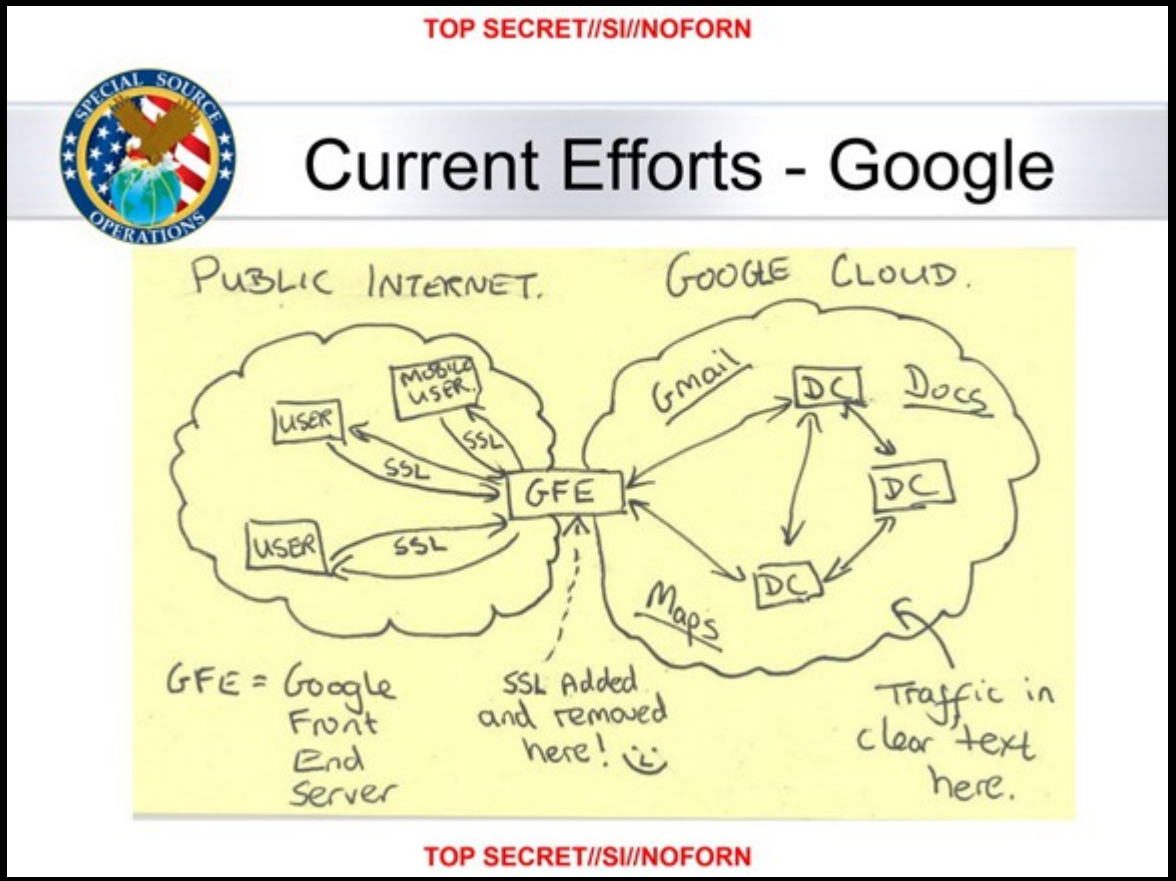
Save the turtles....

Stop Dragnet Surveillance!

TODO #5

Encrypt your data center traffic!!!

Don't be Google/Yahoo/Microsoft!



How do I encrypt inter-server data?

Easy answers: SSH, VPNs

Other answers: IPSec, MPLS encryption

The best choice is going to depend on your scale, circumstances, and engineering resources

Okay, so speaking of network protocols...

TODO #6

TCP, DNS, HTTP, X.509, XMPP...

Our network protocols are not great

There are some proposed improvements in the works...

DNSSEC may make TLS much more secure,
but only if DANE becomes a reality

(meanwhile, DNSSEC is nice but not a magic bullet for anything)

HTTP/2.0 ?

- might require HTTPS (via a CA???)
- might support opportunistic encryption

Opportunistic encryption is a Very Good Idea

Some TCP replacements in the works...
QUIC, MinimalT

Lots of people are working on more secure and usable successors to PGP and OTR

Here's what we need from these protocols!

- encryption by default
- forward secrecy
- clever, usable authentication
- a security / complexity knob *on the server side*
- design for multiple, roaming devices

Here's what we need from these protocols!

- encryption by default
- forward secrecy
- clever, usable authentication
- a security / complexity knob *on the server side*
- design for multiple, roaming devices
- smart response to evil networks (hotels, 3G, etc)
- extremely good performance (bufferbloat, WiFi noise)
- pseudonymity-friendly, identity based addressing

Now is a very hard and very interesting time to be working on network protocols!

TODO #7

https://eff.org/donate

https://eff.org/jobs