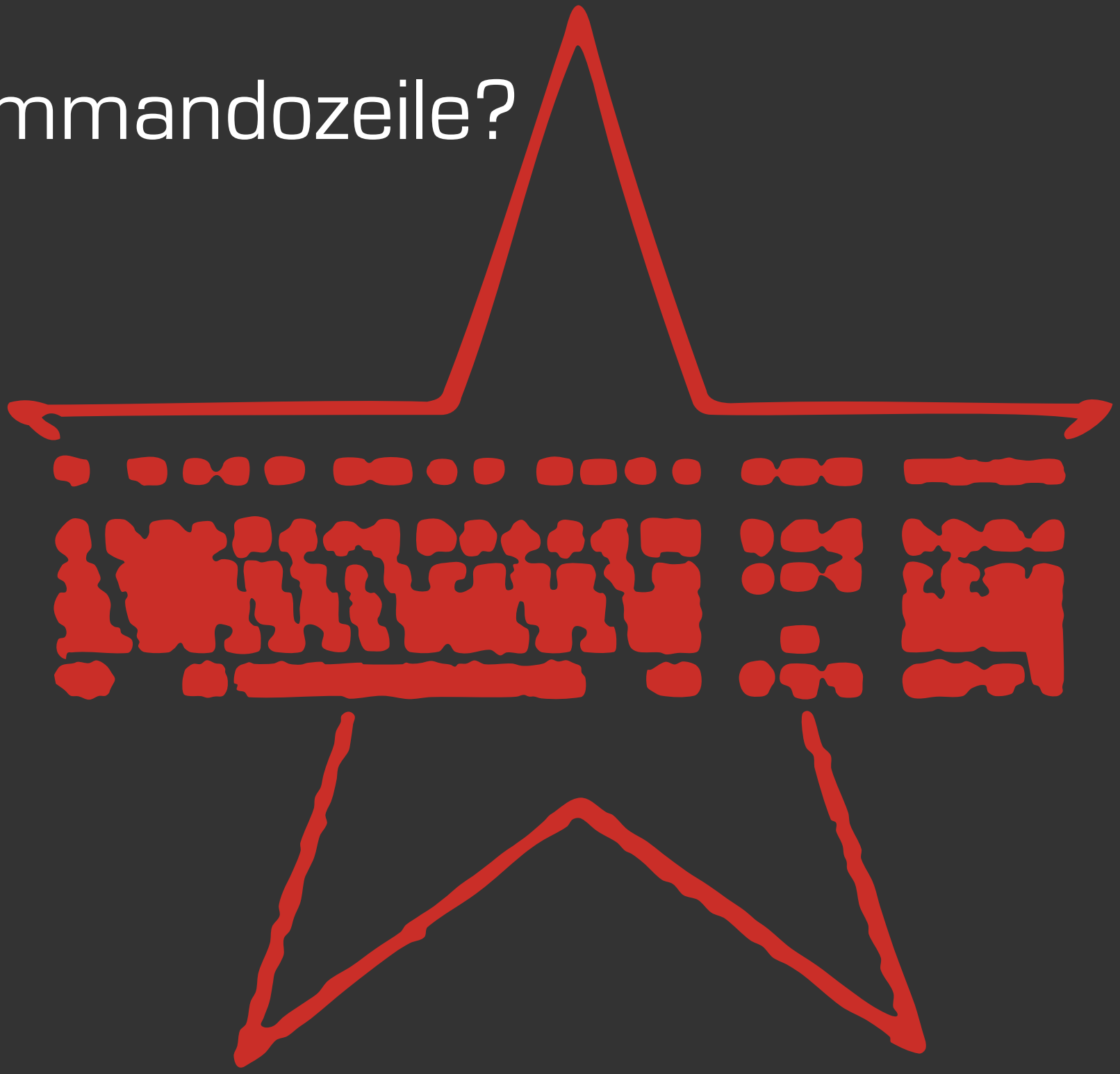
sva@ccc.de

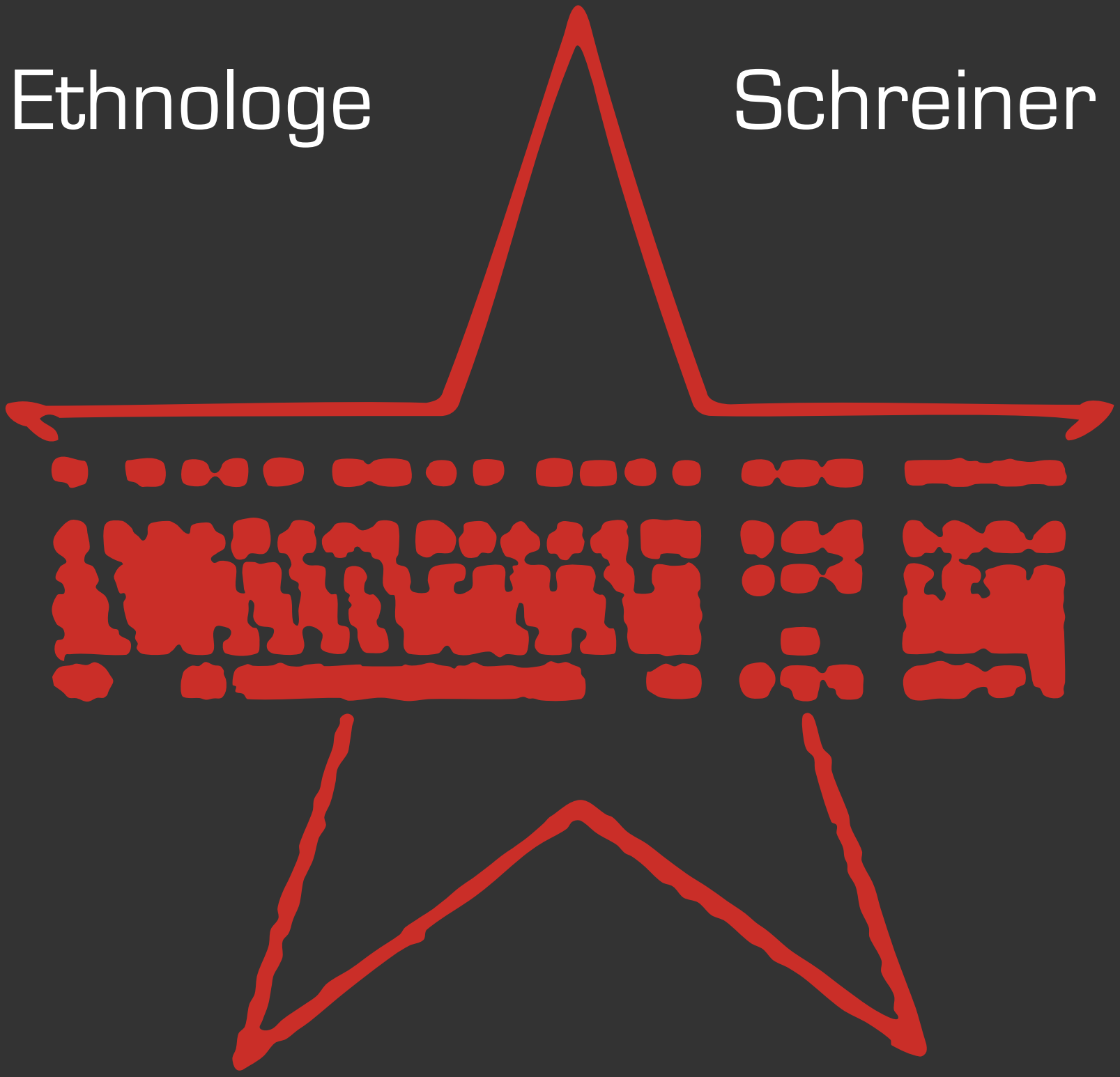
twitter@sva

Kommandozeile?



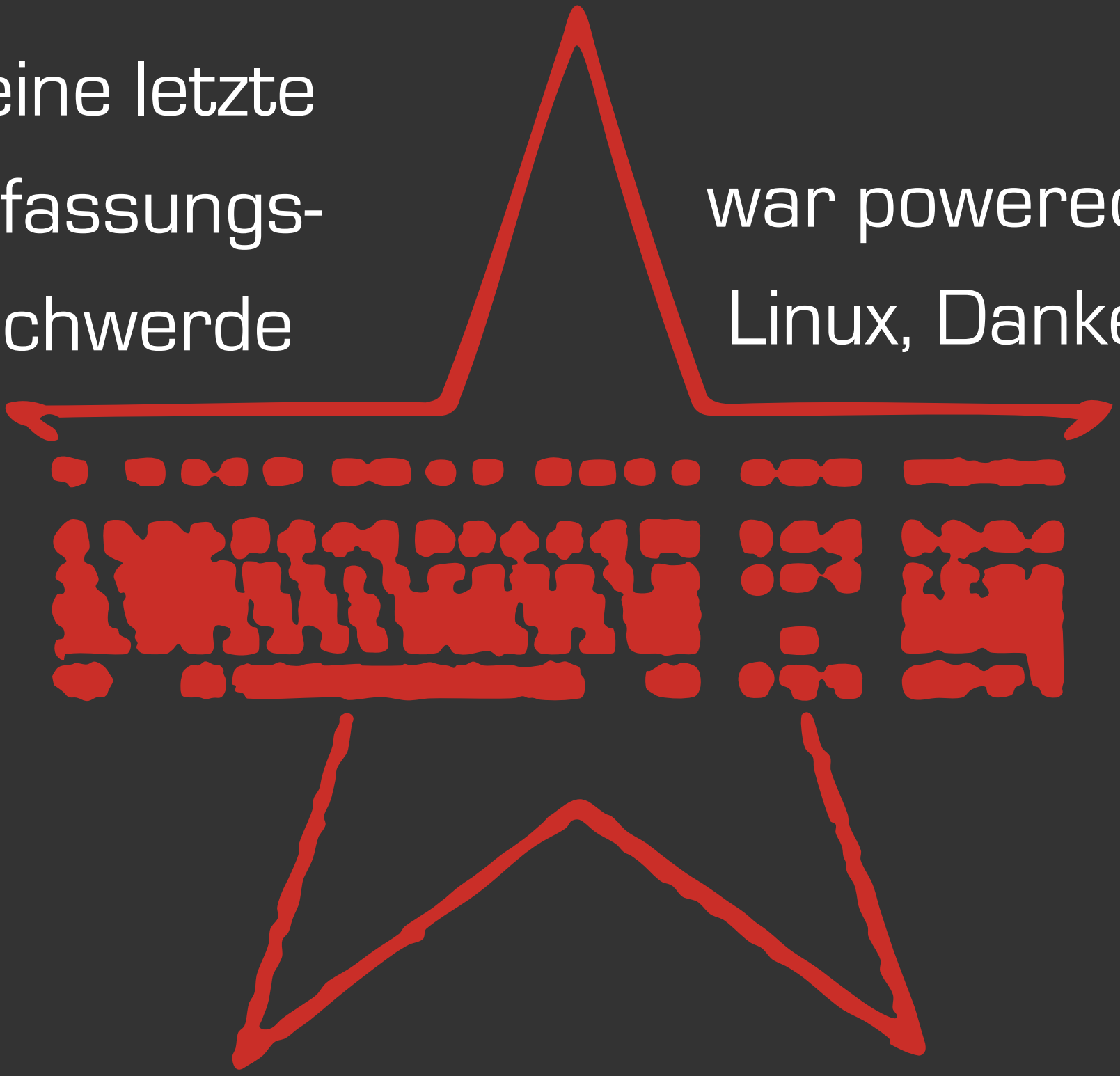
Ethnologe

Schreiner



Einführungsvortrag vom letzten Jahr?

“meine letzte Verfassungs-beschwerde



war powered by Linux, Danke!”

Software ist

Magie

Technik ist

Magie

Wir sind die

Magier!

Wie man einen Wahlbetrug erkennt:

Dies ist ein Wahlcomputer

Dies ist ein manipulierter Wahlcomputer

2008

Wir sind die

Magier!

...und

Missionare?

Technikverständnis

“Merkste was?”

Alle können

das verstehen

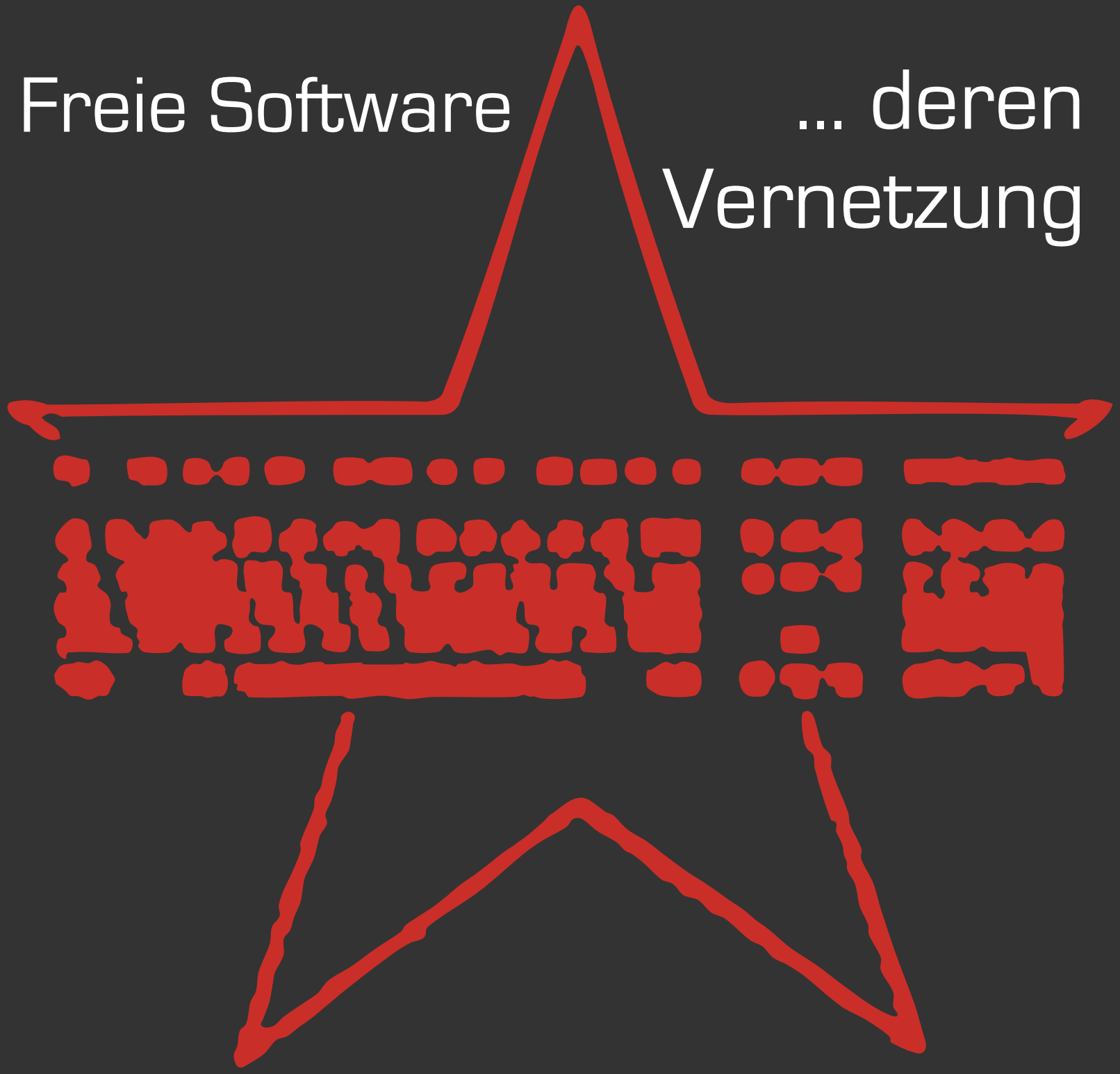

Bescheiden?
Arrogant?

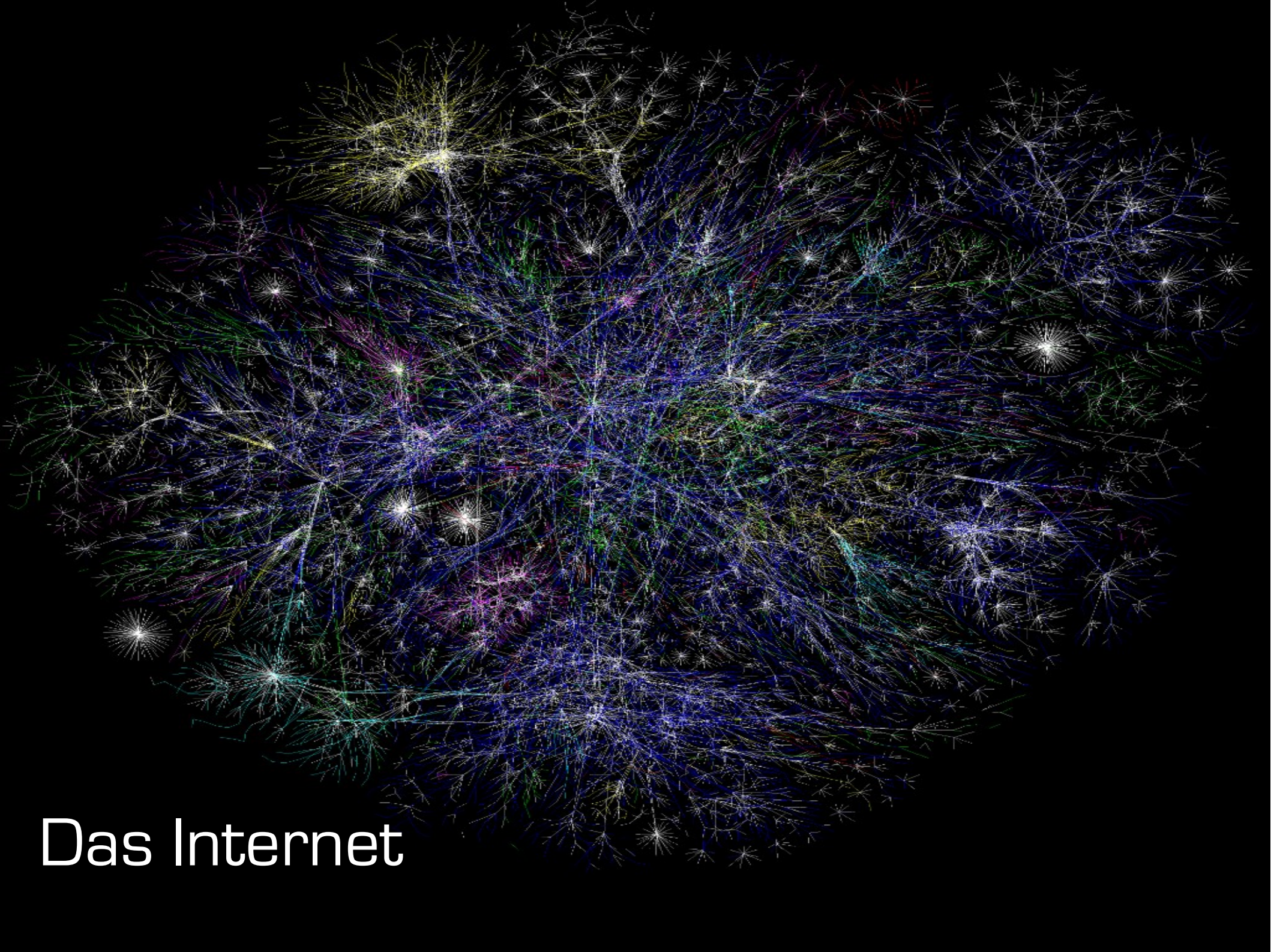
Egal.

Die anderen machen uns zu Magiern...

Freie Software

... deren Vernetzung




Das Internet

2013

Verschlüsselung!
Überall, alles, immer!
Massenverschlüsselung!

Metadaten?
Öhm...

Symptome...?

Langfristige Lösungen!

Ethnologen haben “Zugang zum gesamten Datenbestand von Facebook”

https://www.heise.de/tr/artikel/Voelkerkunde-bei-Facebook-1777442.html

...können Empfänger-gruppe manipulieren!

https://www.heise.de/tr/artikel/Voelkerkunde-bei-Facebook-1777442.html

Cambridge Analytica

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

“Psychometrie, manchmal auch Psychografie genannt, ist der wissenschaftliche Versuch, die Persönlichkeit eines Menschen zu vermessen.”

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

2012 nachgewiesen: Mit durchschnittlich 68 Facebook-Likes kann man vorhersagen:

welche Hautfarbe (95%)
Homosexualität (88%)
Demokrat oder Republikaner (85%)

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Intelligenz
Religionszugehörigkeit
Alkohol-, Zigaretten- und Drogenkonsum

Ob die Eltern einer Person bis zu deren 21.
Lebensjahr zusammengeblieben sind,
oder nicht.

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Vorhersagen besser wie...

...Arbeitskollege: 10 Likes
...Freund: 70 Likes
...Eltern: 150 Likes
...Partner: 300 Likes

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

“...mit noch mehr Likes lässt sich sogar übertreffen, was Menschen von sich selber zu wissen glauben.”

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

“Am Tag, als Kosinski diese Erkenntnisse publiziert, erhält er zwei Anrufe. Eine Klageandrohung und ein Stellenangebot. Beide von Facebook.”

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Grundbucheinträge
Bonuskarten
Wählerverzeichnisse
Clubmitgliedschaften
Zeitschriftenabonnements
Medizinische Daten

& Daten von global tätigen Datenhändlern

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

“Wir haben Psychogramme von allen erwachsenen US Bürgern – 220 Millionen Menschen”

Alexander Nix, CEO Cambridge Analytica

https://www.youtube.com/watch?v=n8Dd5aVXLCc

The Second Amendment isn't just a right. **It's an insurance policy.**

DEFEND THE RIGHT TO BEAR ARMS

From father to son

Since the birth of our n

DEFEND THE SECOND AMENDMENT

https://www.youtube.com/watch?v=n8Dd5aVXLCc

Wahlhelfer klingeln nur, wenn die Leute als empfänglich eingestuft wurden – natürlich mit passendem Gesprächsleitfaden.

https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Datensammlungen ^

Datenpunkte sammlen >

Frank Rieger & Thorsten Schröder, 2016

https://re-publica.com/en/16/session/ad-wars-ausflug-realitat-online-werbung

Nachrichtenportale 2 Min rumgeklickt:

Startseite + 3-4 Artikel + 3-4 Rubriken

https://re-publica.com/en/16/session/ad-wars-ausflug-realitat-online-werbung

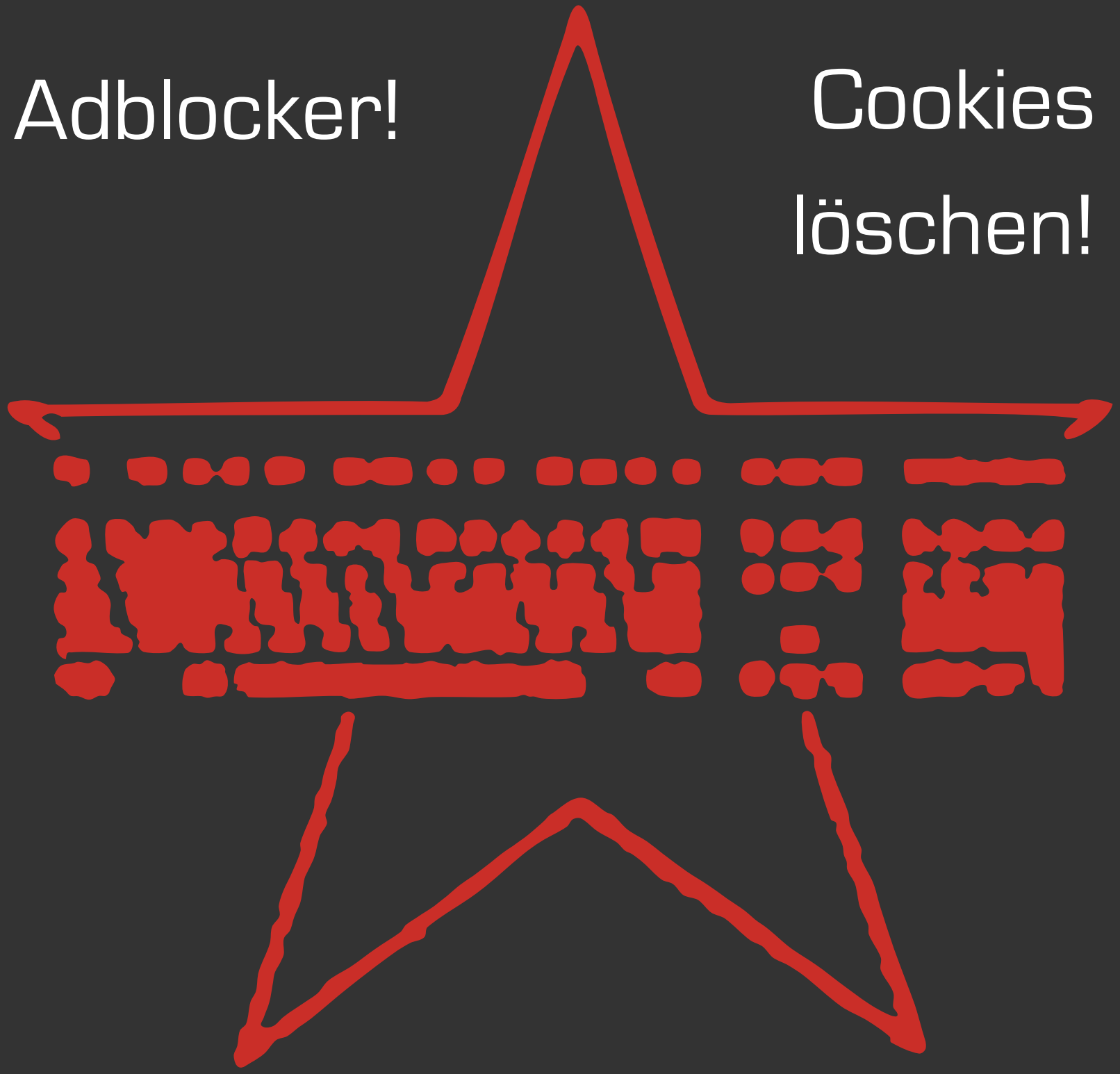
	BILD.DE	SPON	SZ	ZEIT
Requests	2339	2514	1886	1130
Unique Hosts	**195**	**184**	**172**	**122**
3rd Party Hosts	182	172	160	113
Own Hosts (*)	**13**	**12**	**12**	**9**

(*) basiert auf augenscheinlich zum Verlag gehörenden Domains/Subdomains

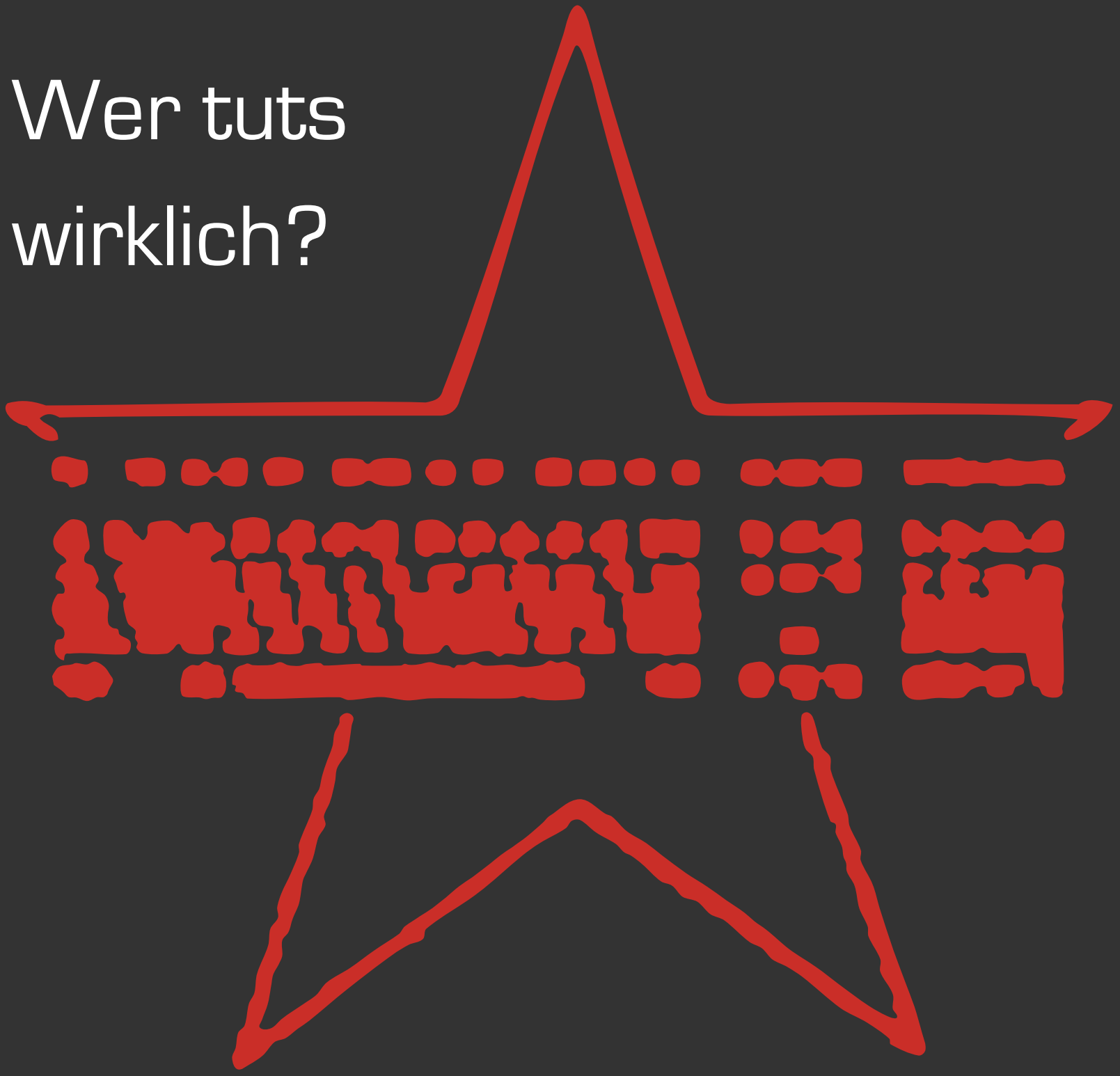
“Ad Wars
Ausflug in die Realität der Online-Werbung”

https://re-publica.com/en/16/session/ad-wars-ausflug-realitat-online-werbung

Realität


Adblocker!
Cookies
löschen!

Wer tuts
wirklich?



Apropos Cookies....

Flugsuche!

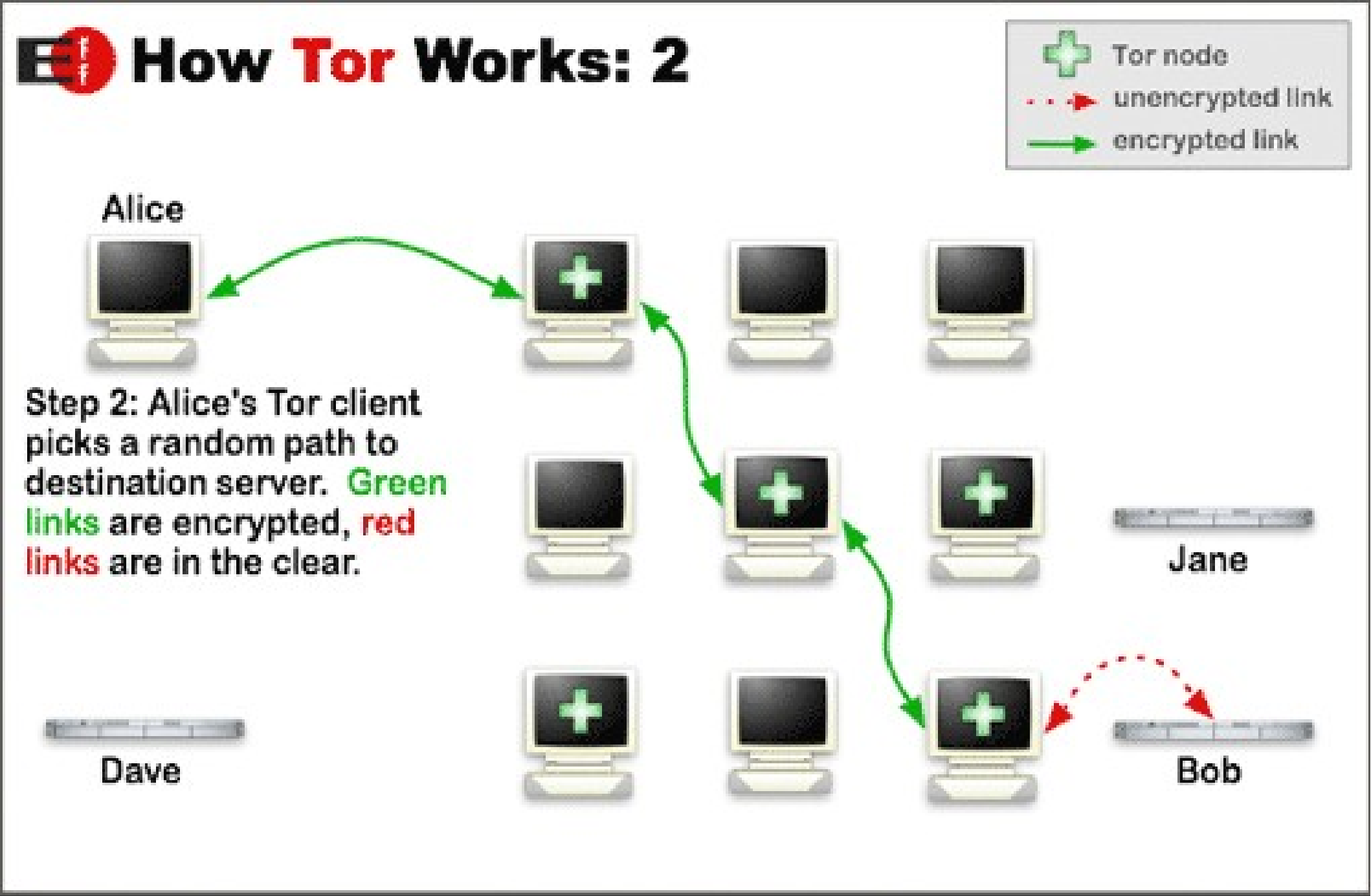
Na gut, ...

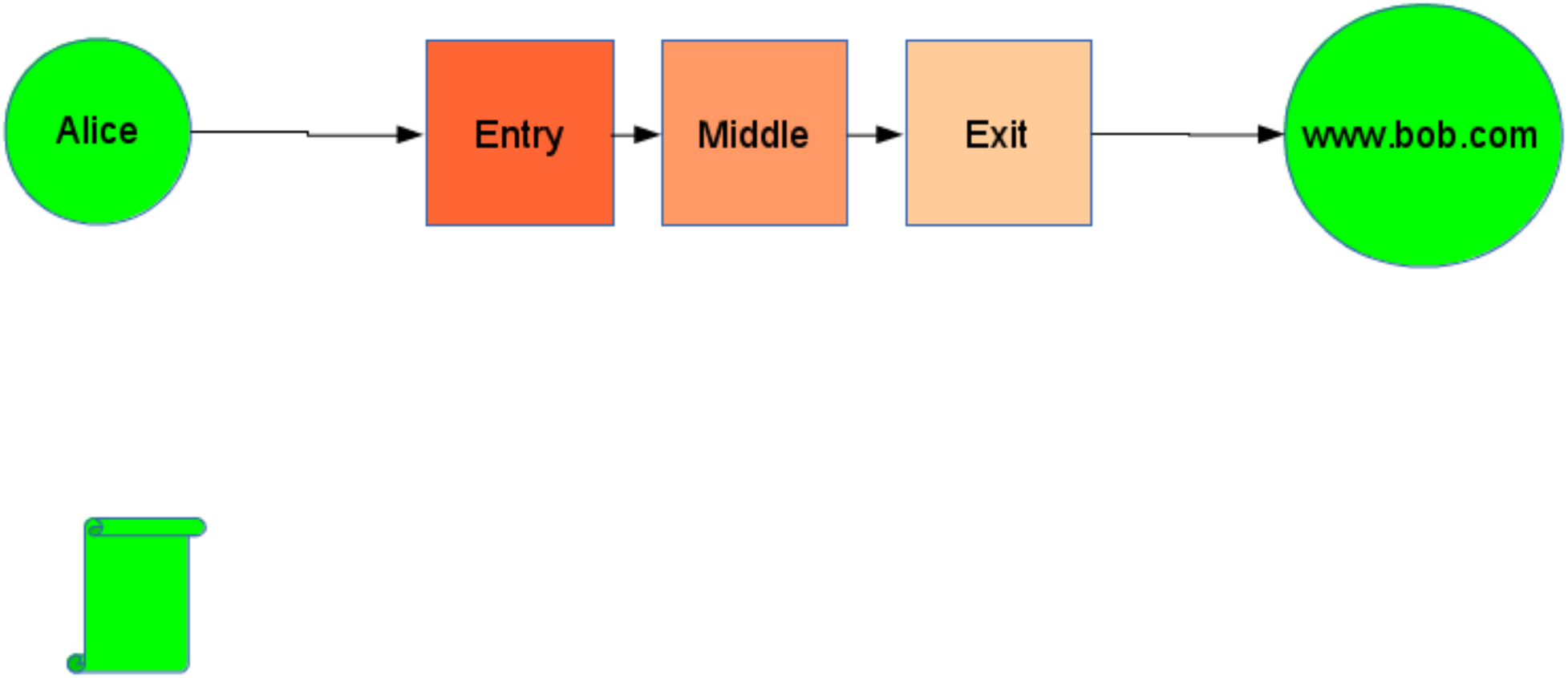
aber Tor!

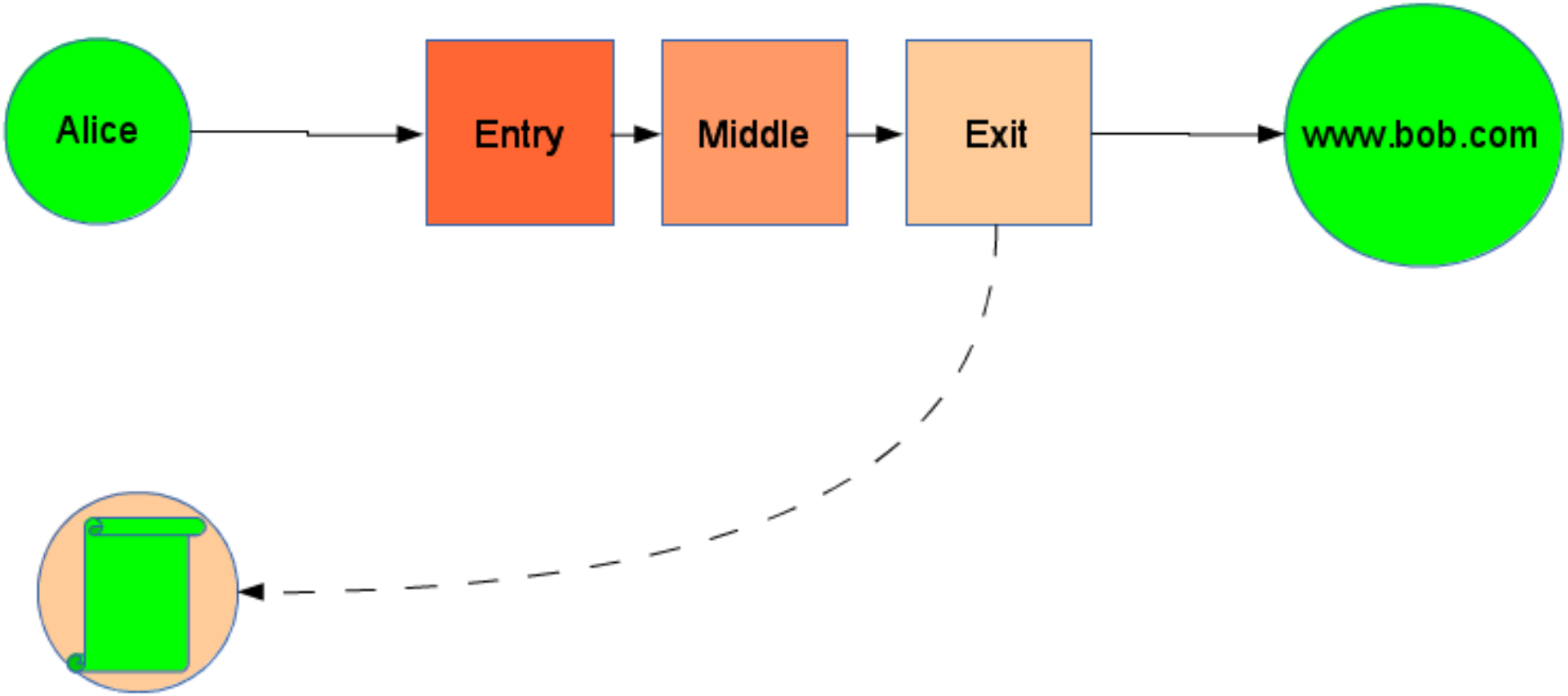
Use Tor!

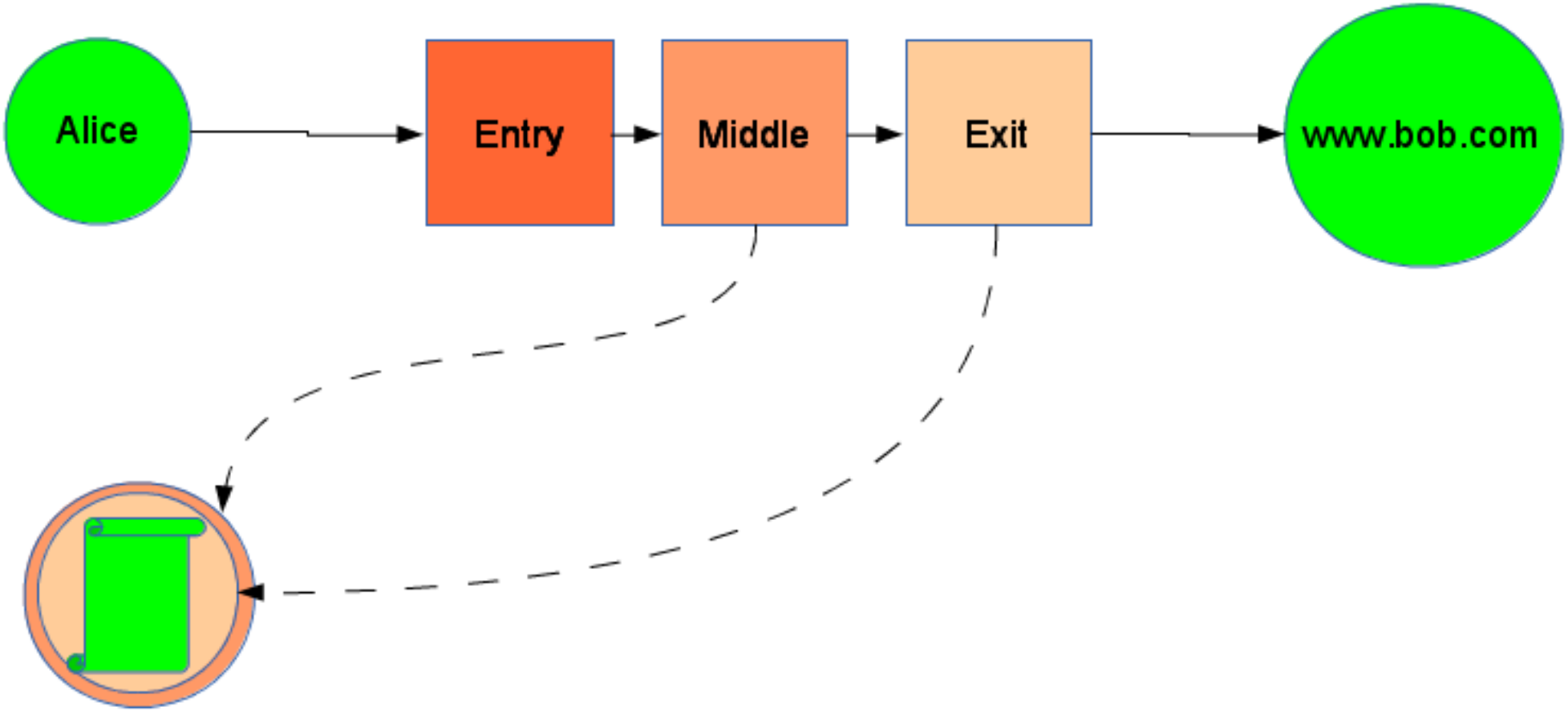
1. Download von torproject.org
2. Installieren
3. Warning Note lesen
4. Benutzen!

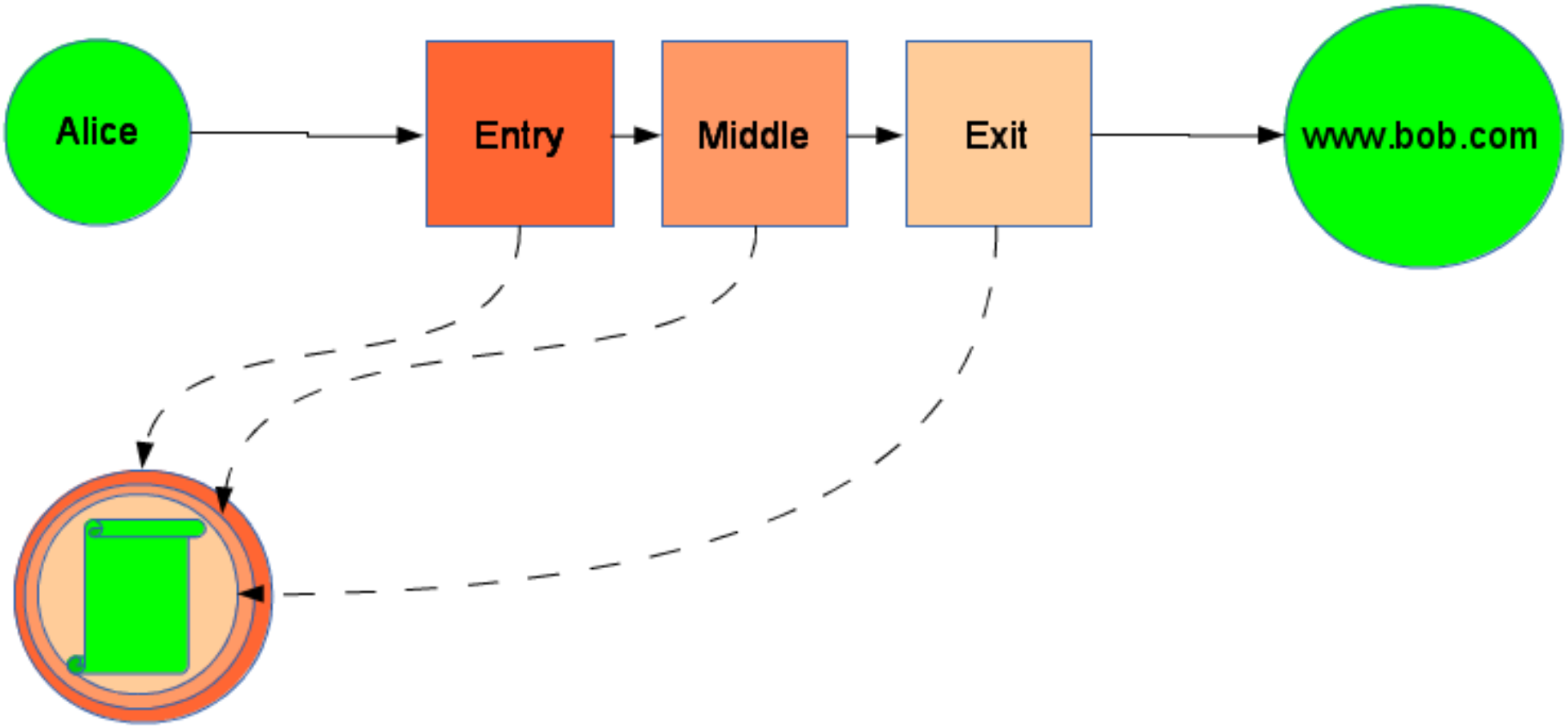
How Tor Works: 2

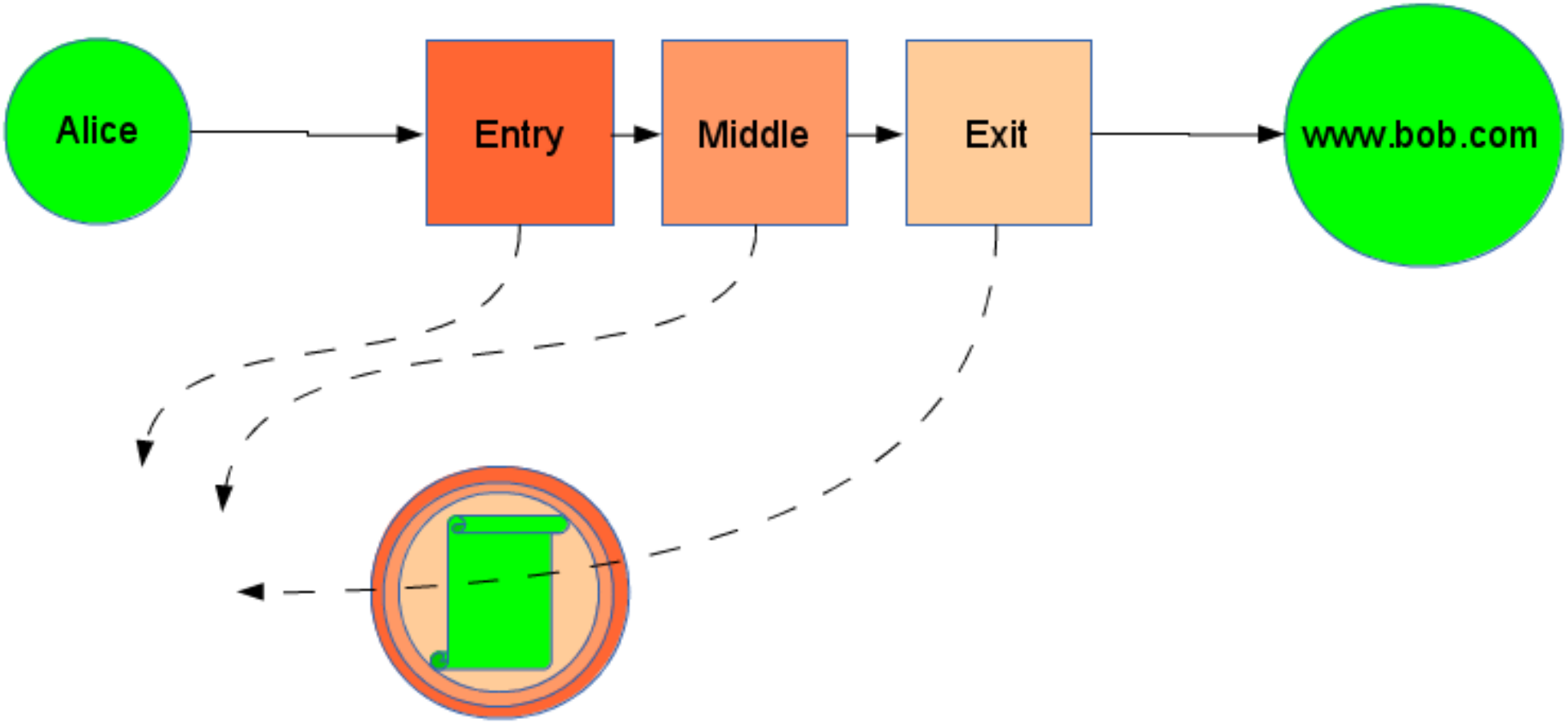


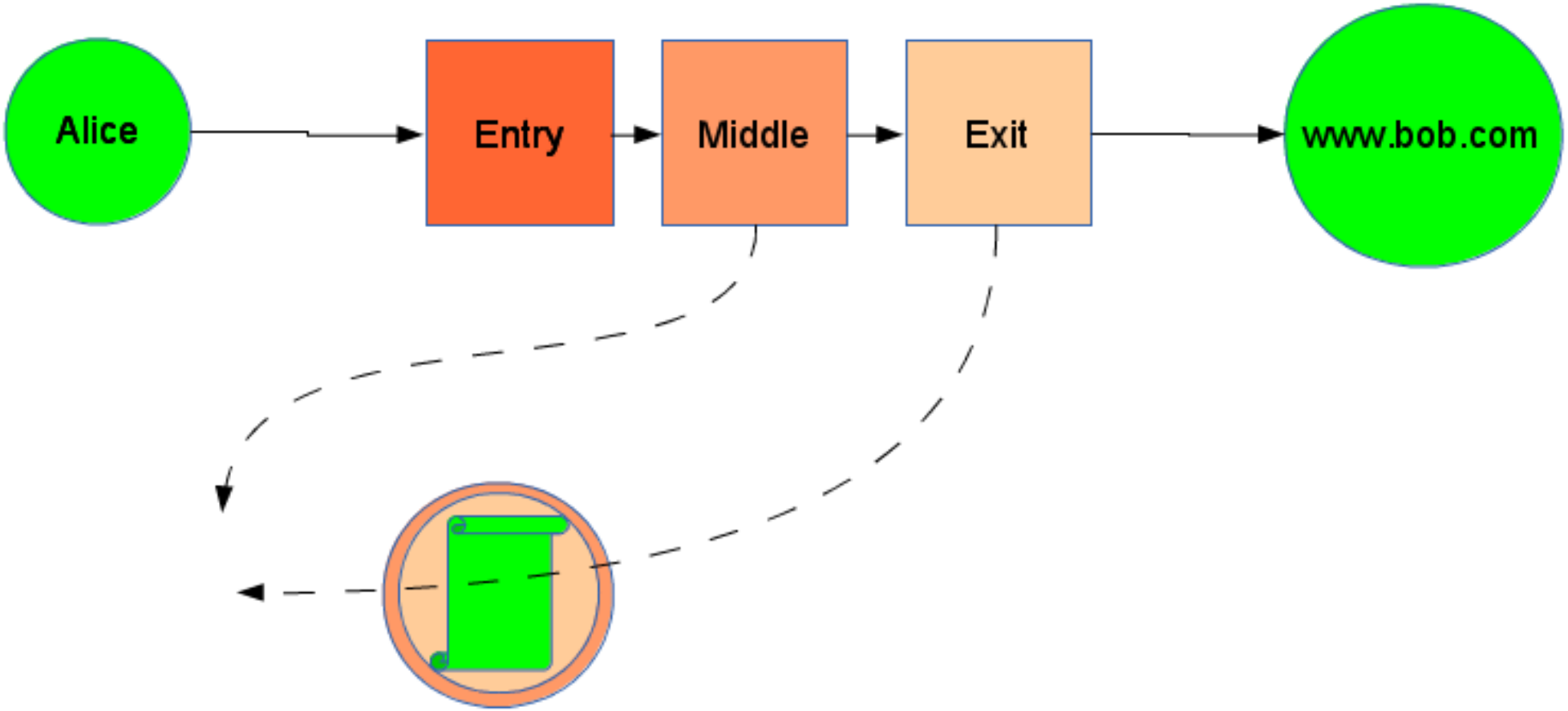

Alice
Entry
Middle
Exit
www.bob.com

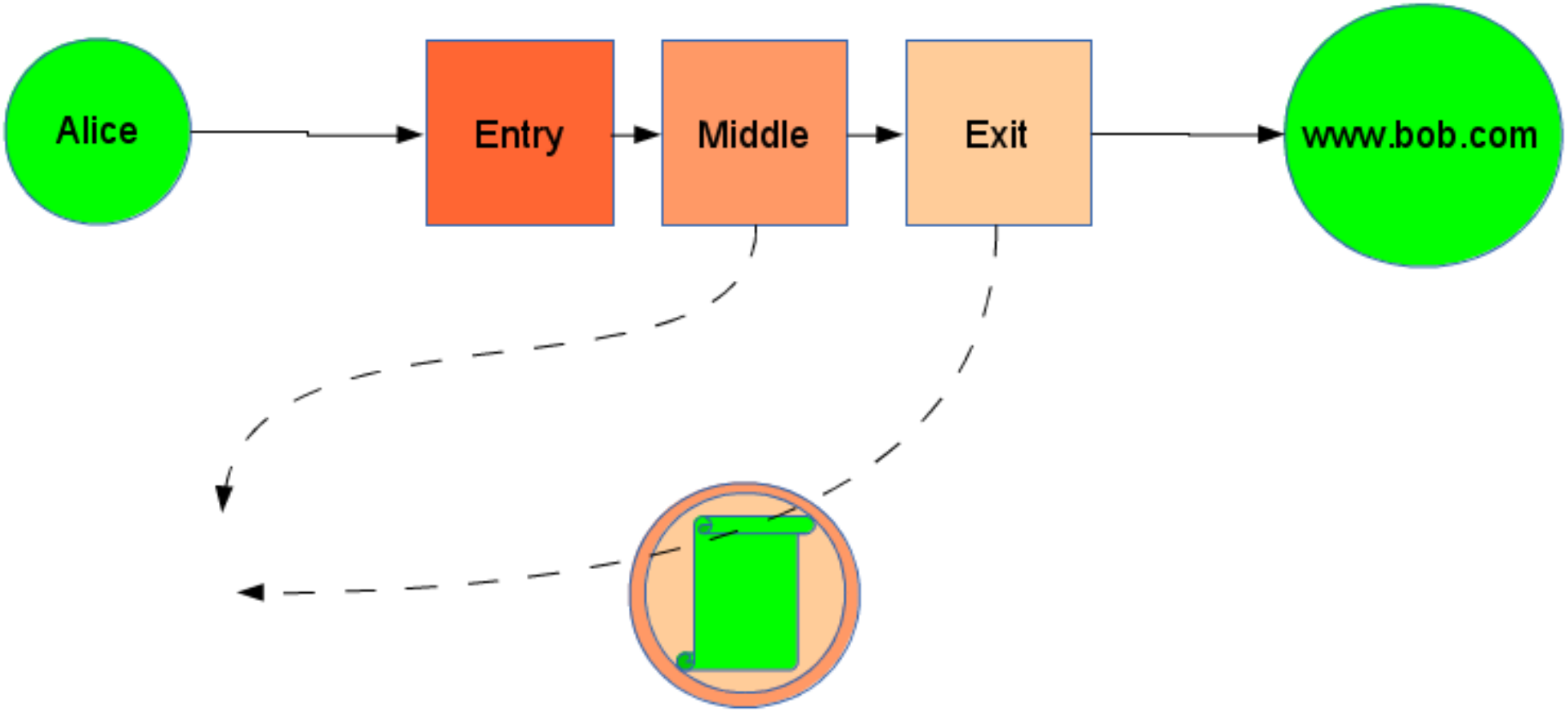

Alice
Entry
Middle
Exit
www.bob.com

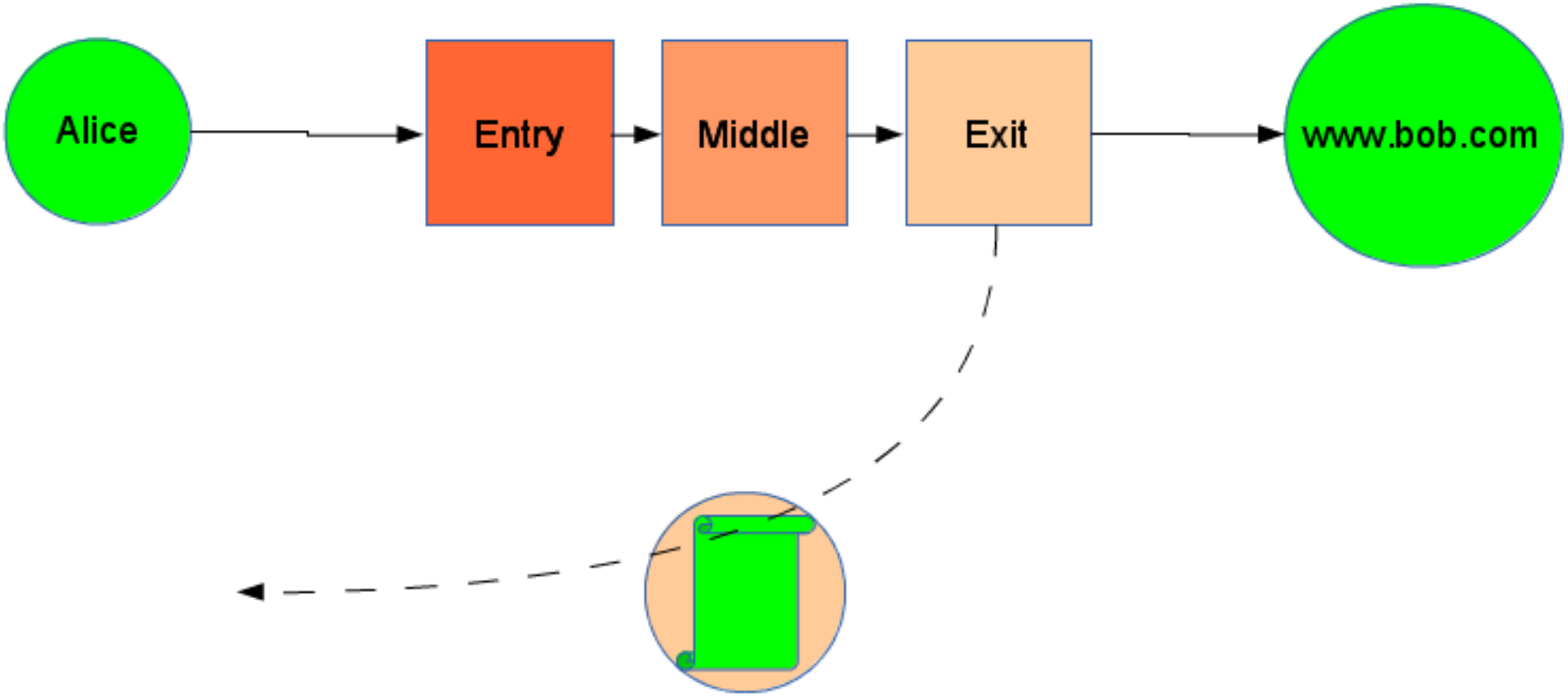

Alice
Entry
Middle
Exit
www.bob.com

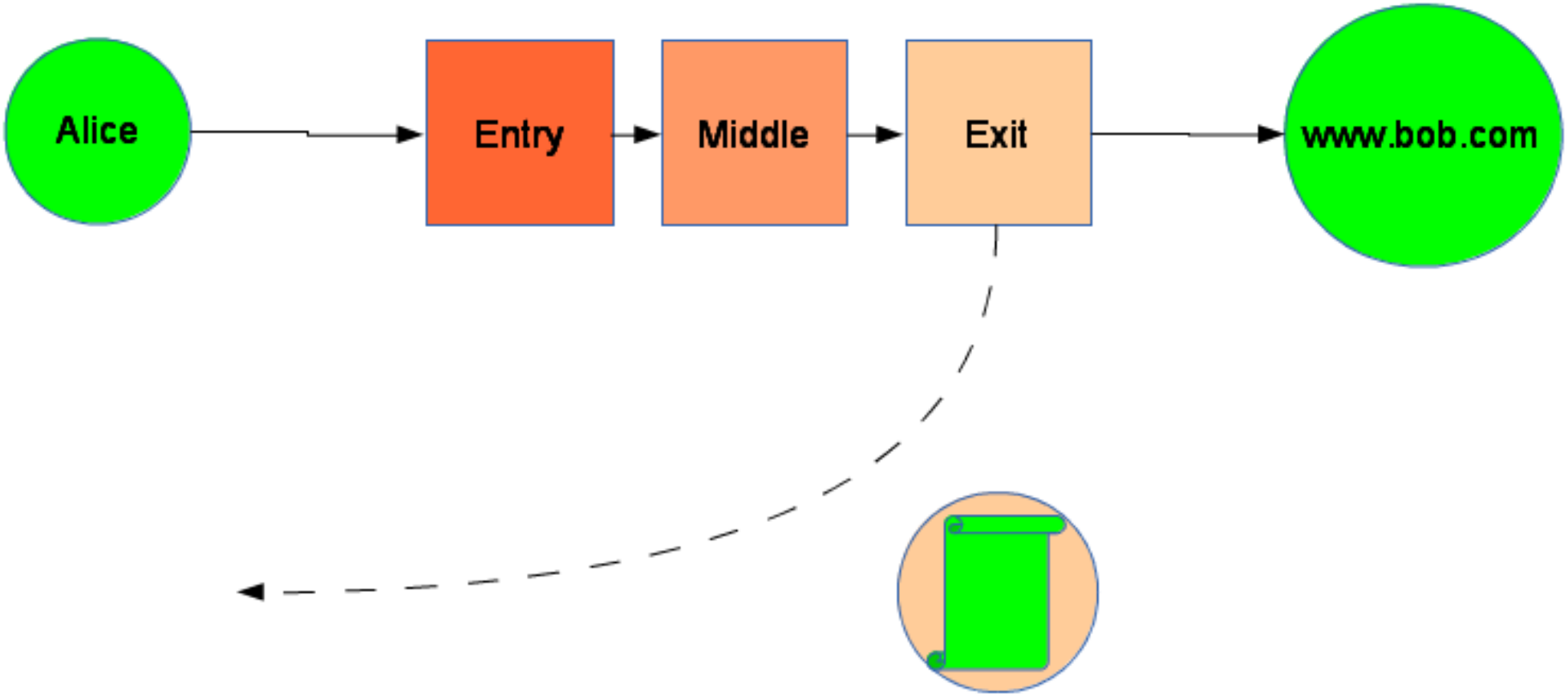

Alice
Entry
Middle
Exit
www.bob.com

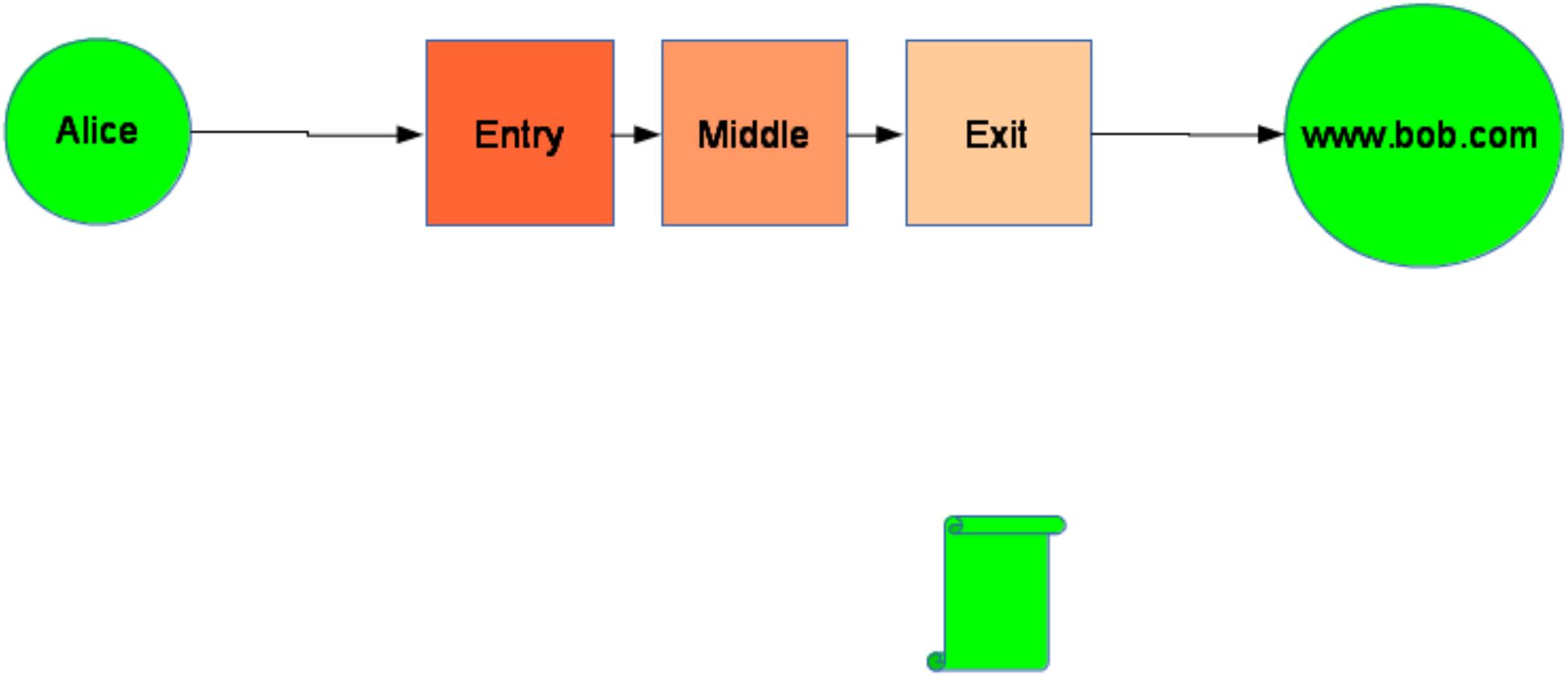

Alice
Entry
Middle
Exit
www.bob.com

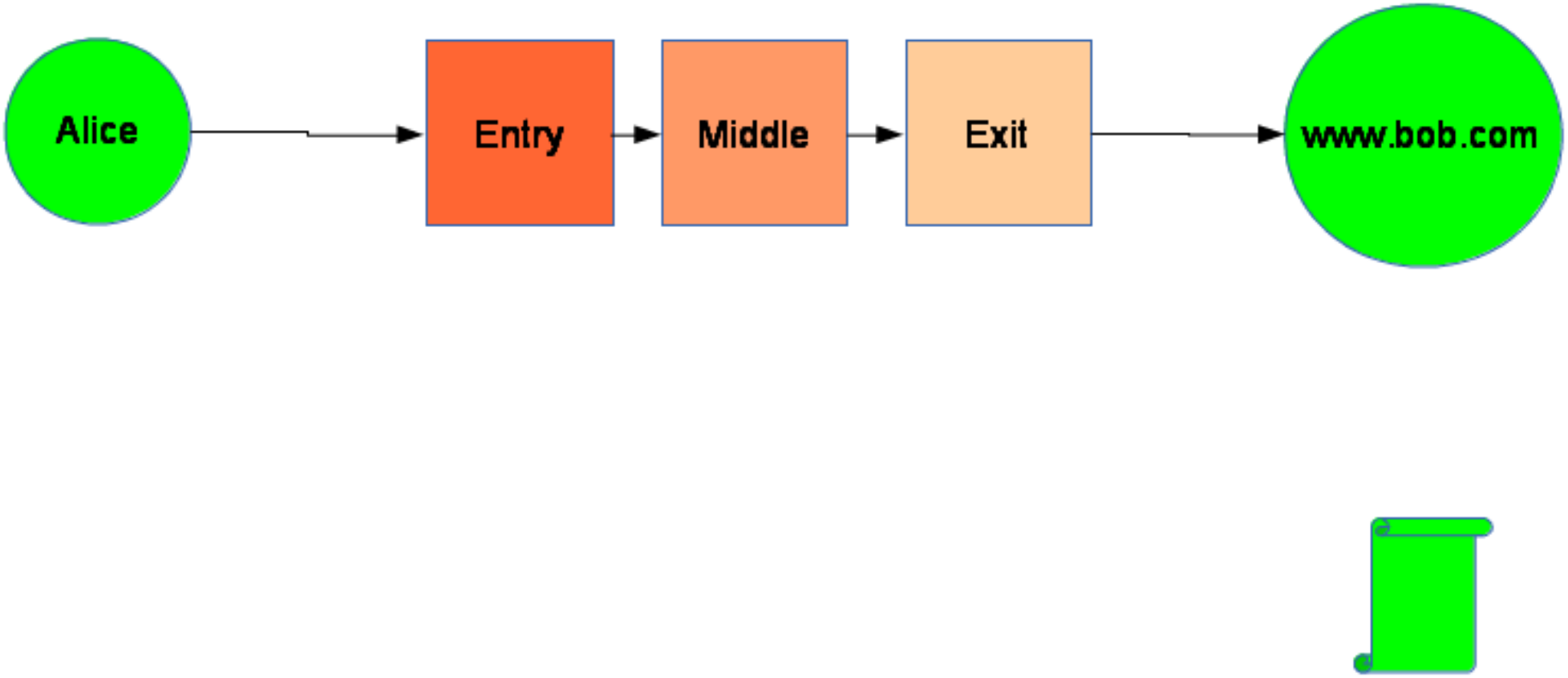

Alice
Entry
Middle
Exit
www.bob.com


Alice
Entry
Middle
Exit
www.bob.com

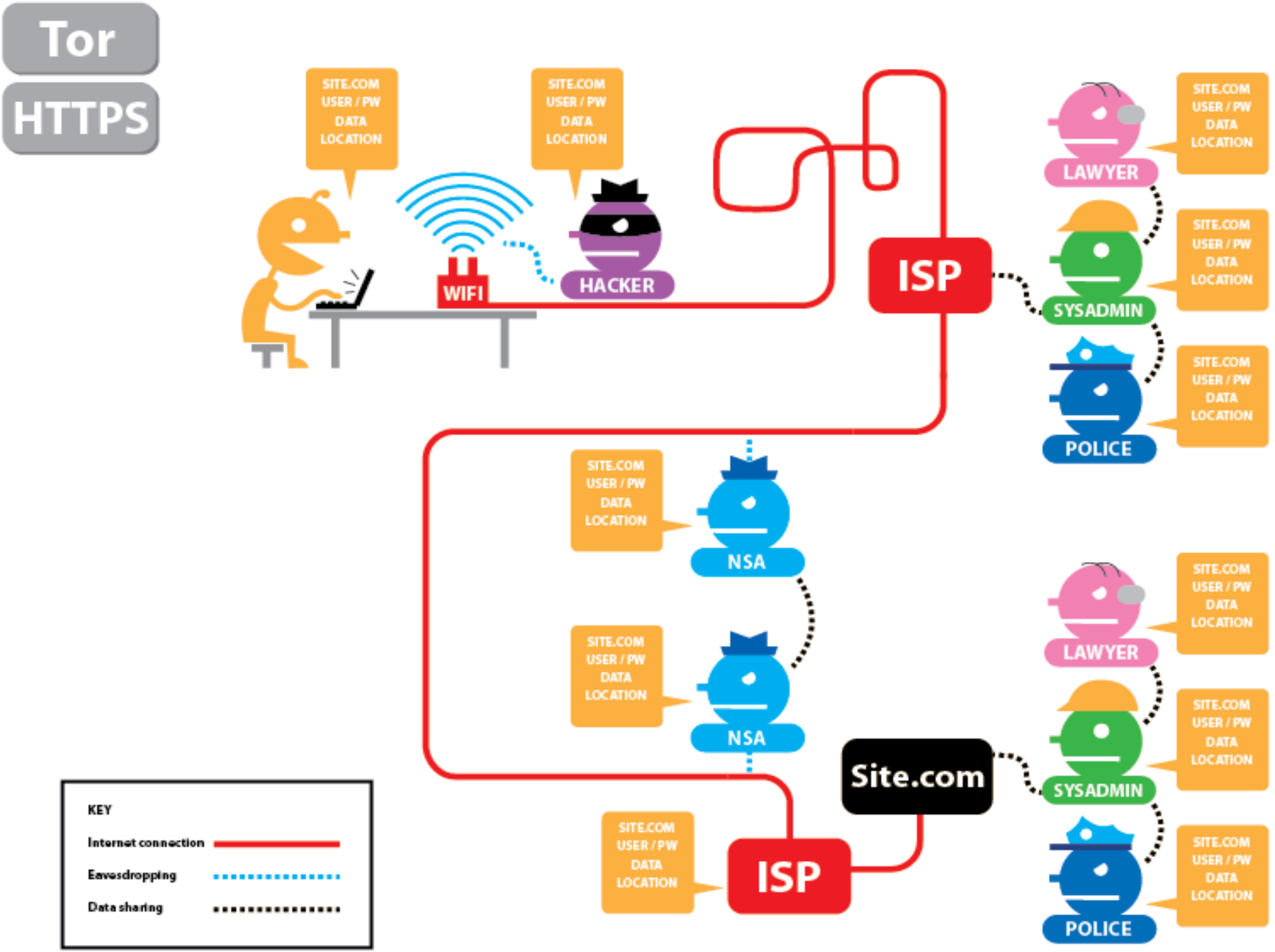

Alice
Entry
Middle
Exit
www.bob.com

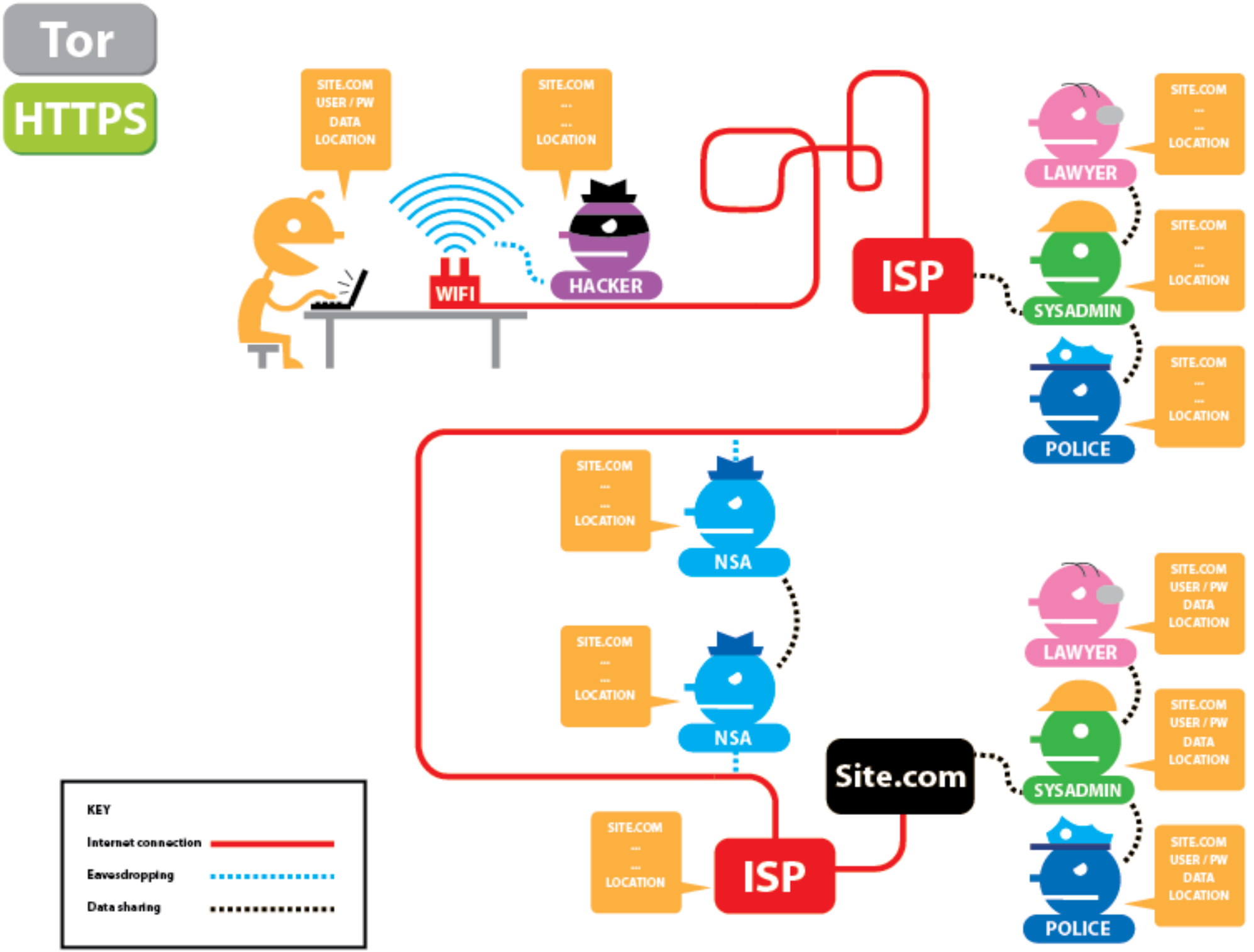

Alice
Entry
Middle
Exit
www.bob.com

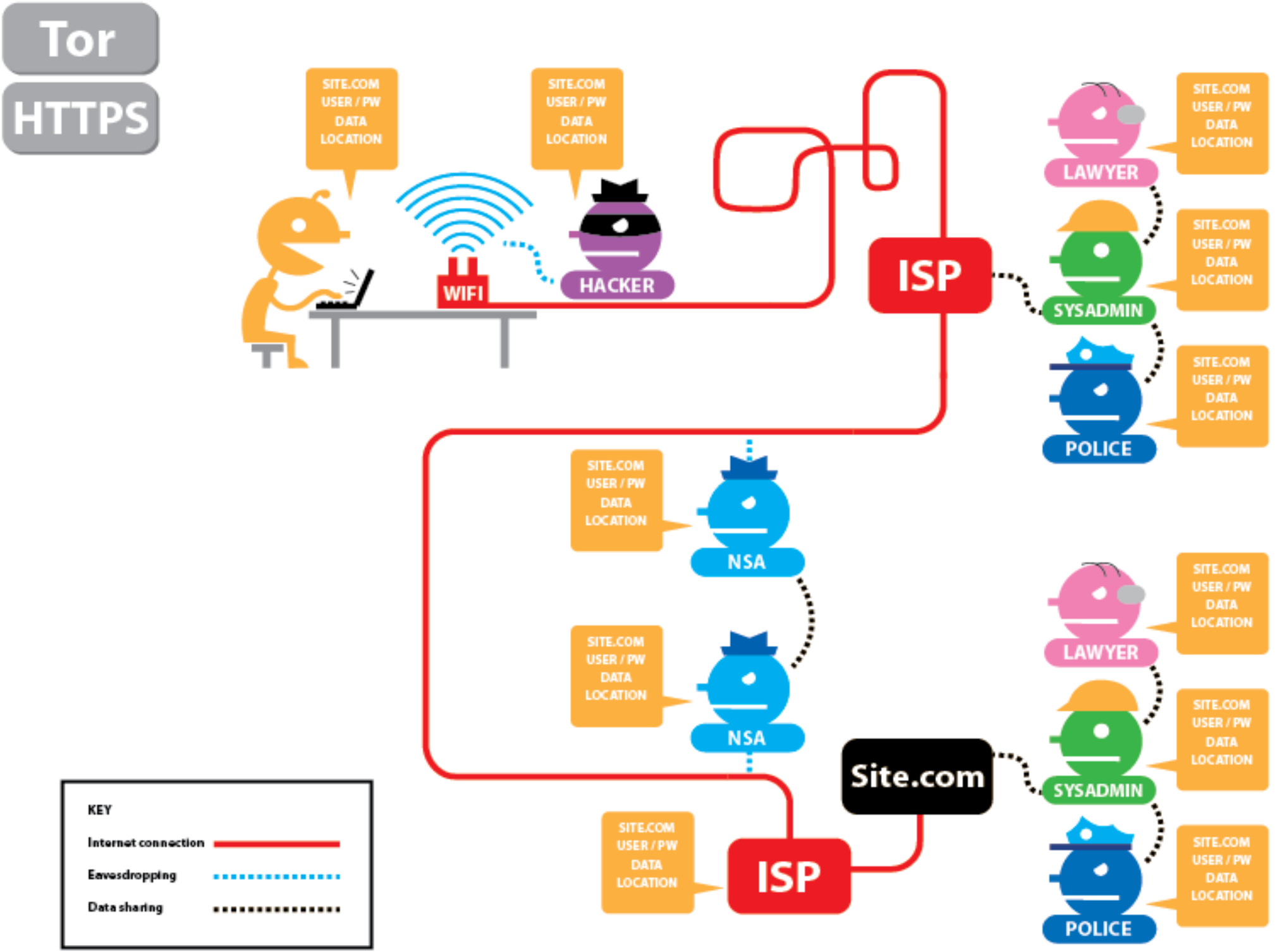

Alice
Entry
Middle
Exit
www.bob.com

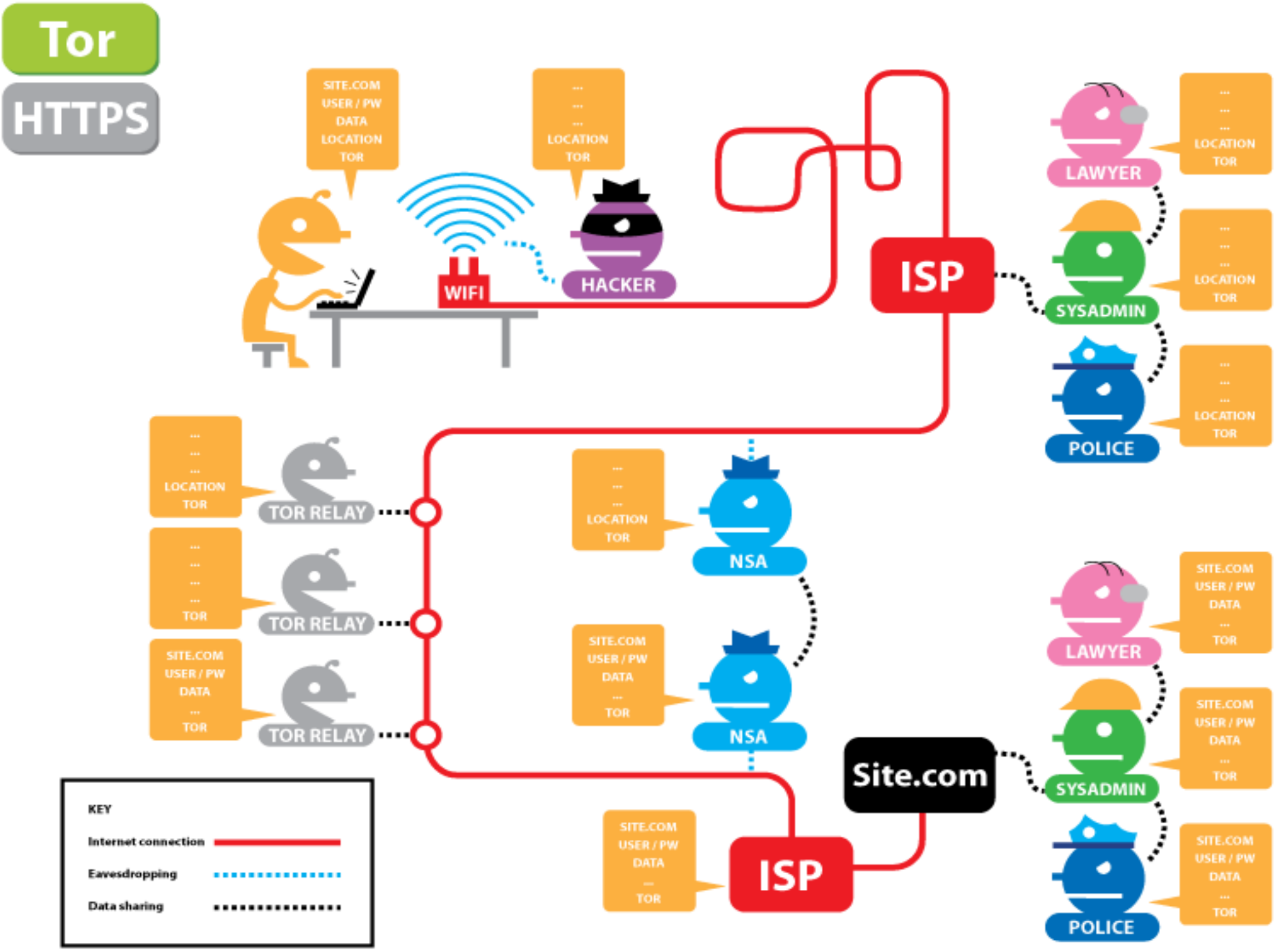

Alice
Entry
Middle
Exit
www.bob.com

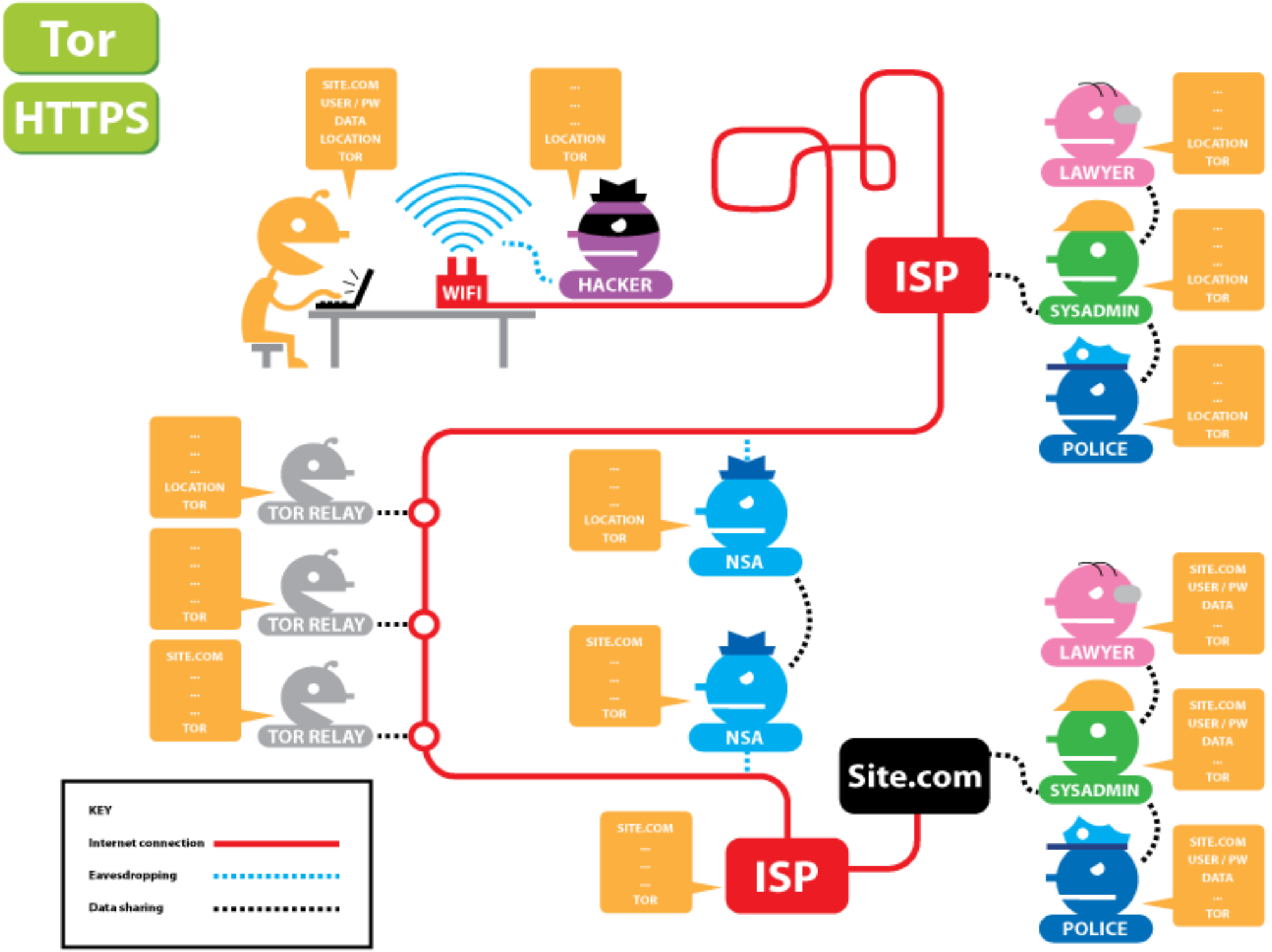
YES
WE SCAN


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
USER / PW
DATA
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
SITE.COM
USER / PW
DATA
LOCATION
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
...
...
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

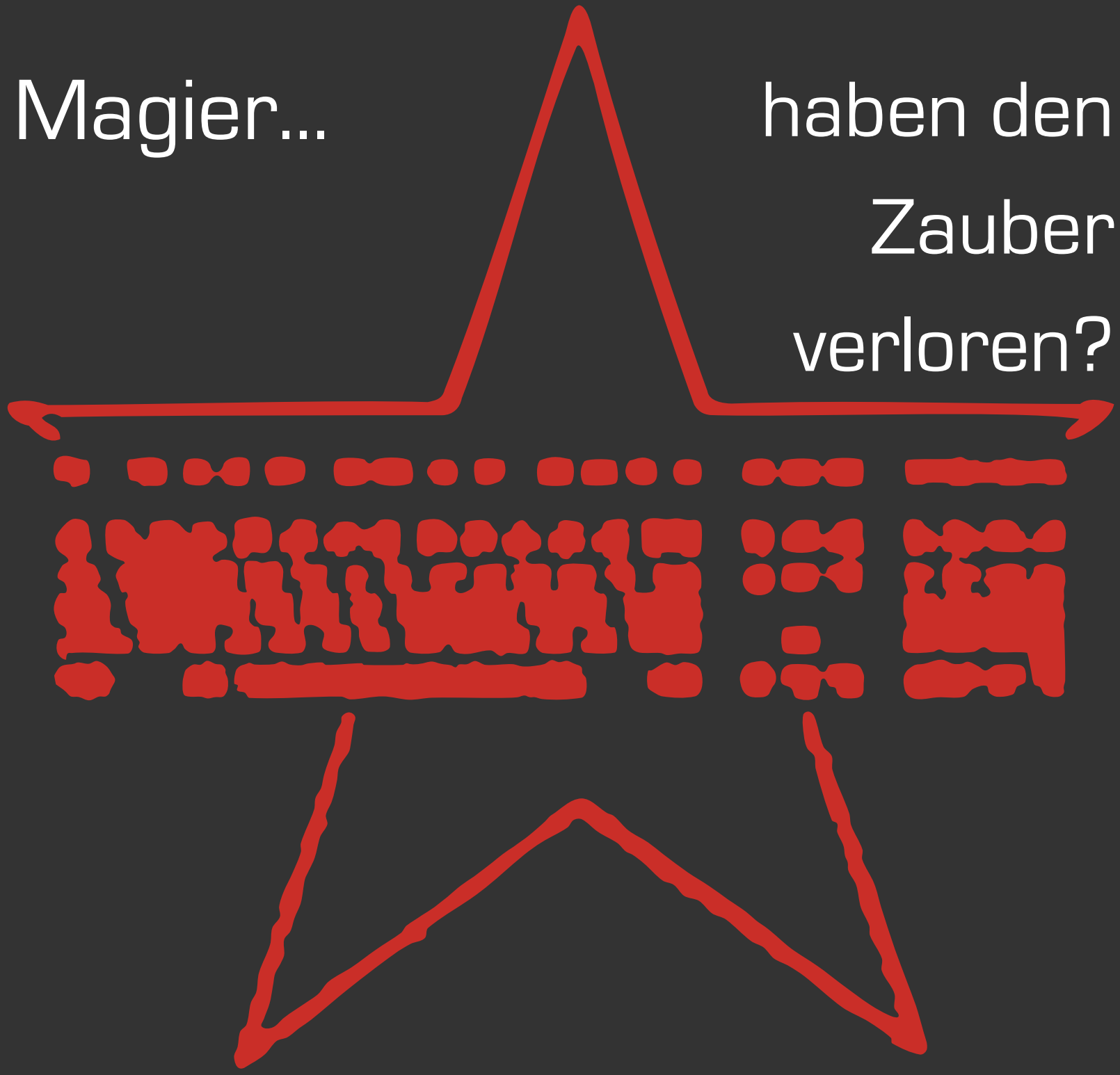

Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
SITE.COM
USER / PW
DATA
LOCATION
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
SITE.COM
USER / PW
DATA
LOCATION
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
...
...
...
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing


Tor
HTTPS
SITE.COM
USER / PW
DATA
LOCATION
TOR
...
LOCATION
TOR
WIFI
HACKER
ISP
LAWYER
SYSADMIN
POLICE
TOR RELAY
TOR RELAY
TOR RELAY
NSA
NSA
Site.com
ISP
KEY
Internet connection
Eavesdropping
Data sharing

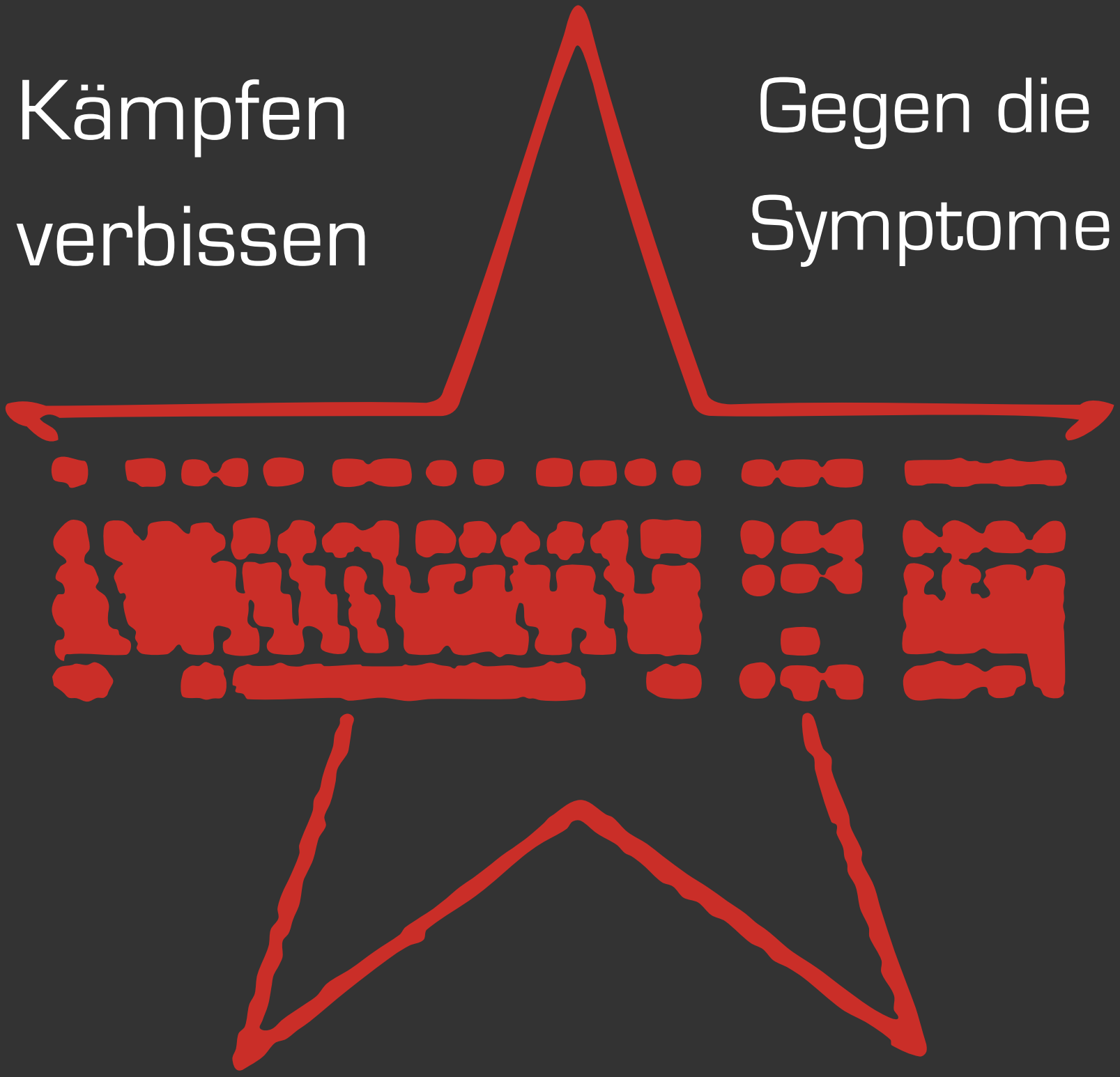
Magier...

haben den Zauber verloren?



Kämpfen
verbissen

Gegen die
Symptome



Apropos
verbissen....

Ursachen-
bekämpfung

Langwierig &
gemeinsam.

Gemeinsam!

Zusammen-
halten

events,
hackspaces,
trust!

Zusammen-
halten

Auseinander-
halten


CHAOS COMPUTER
CLUB
NIX AUF DIE LANGE DATENBAN SCHIEBEN
Hacking is not a crime
POTENTIELL STÖRENDER GEFÄHRDER
SAMMEL-ALBUM 2.0
hat einen KERN-BEREICH
WO BLEIBT EIGENTLICH DIE REVOLUTION?

Beispiele:

Wahlcomputer
Ethnologenforscher manipulieren FB
Cambridge Analytica manipuliert...
Zeitungen verraten ihre Leser

Problem:

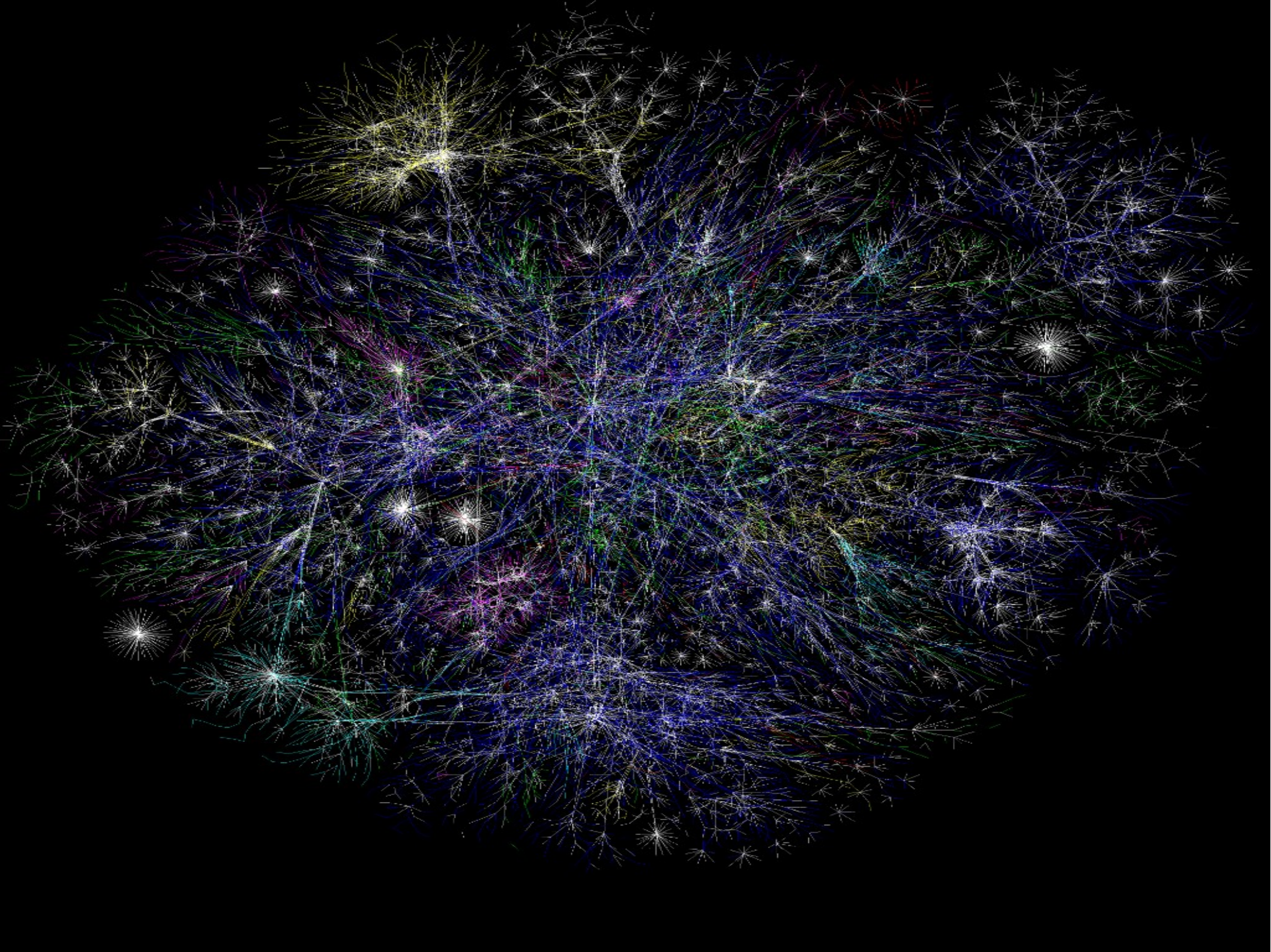
IF

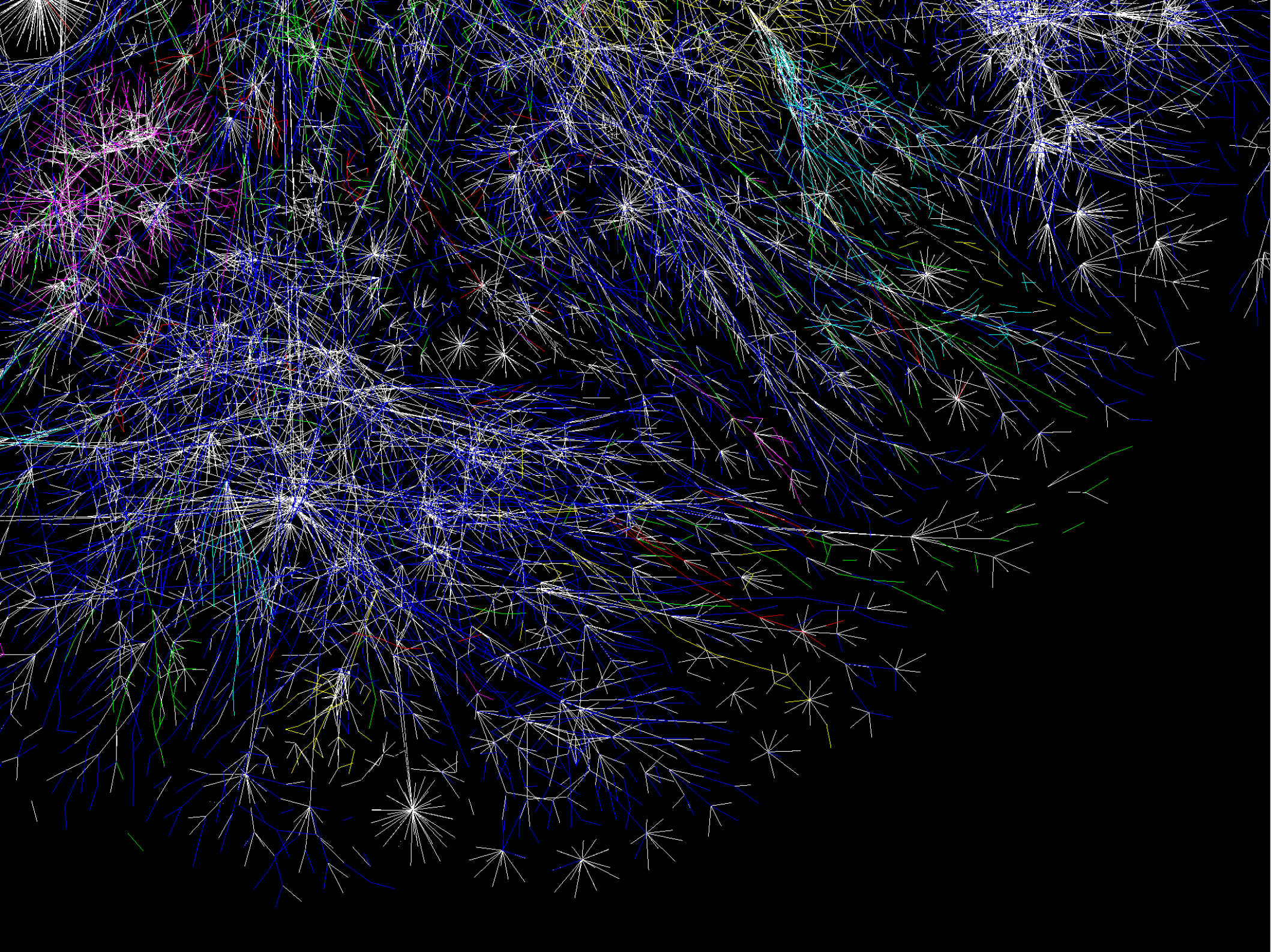
you are connected to the Internet

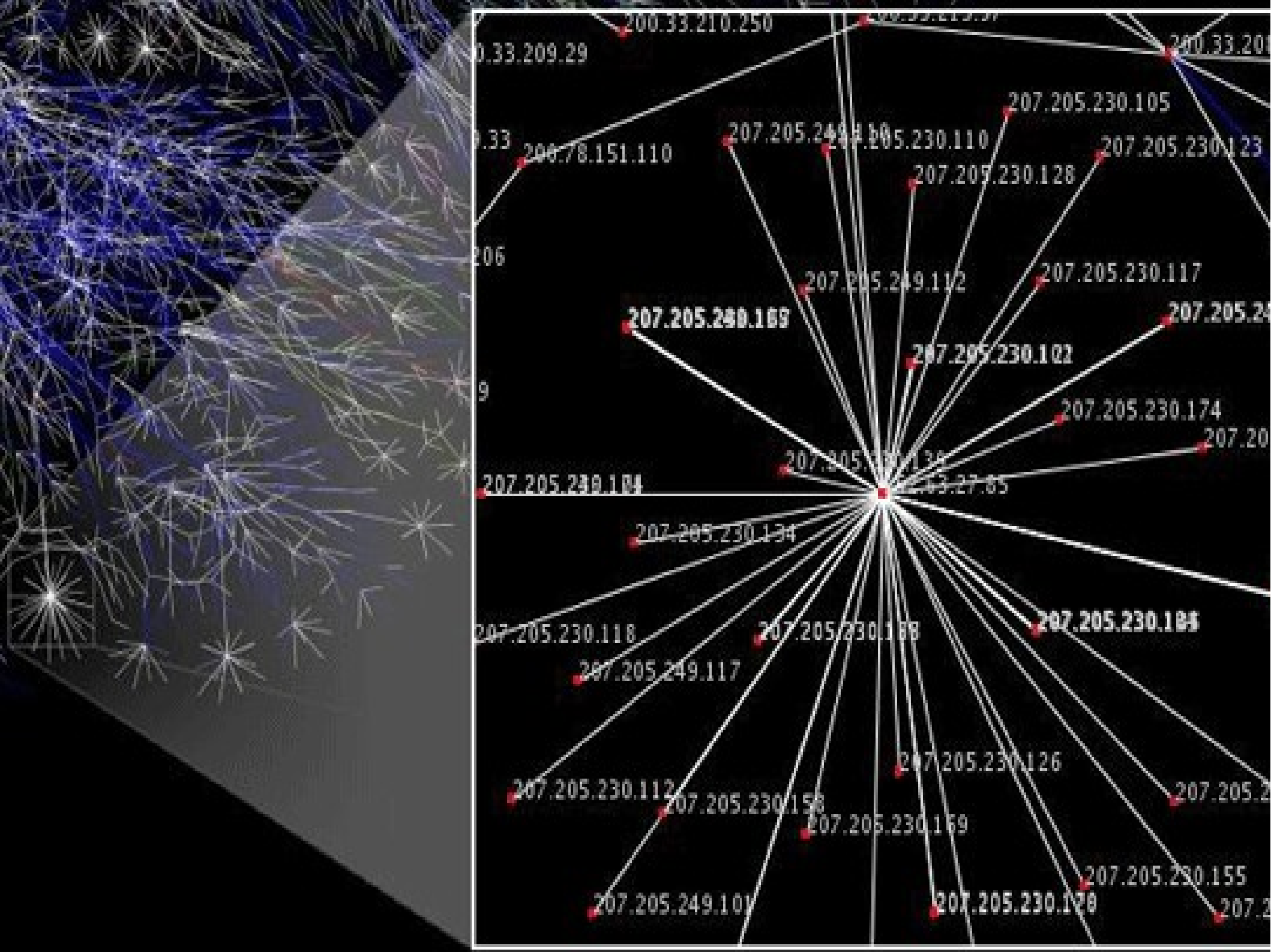
THEN

the Internet is connected to you!

=> you are a part of this network-of-networks






207.205.230.105
207.205.230.110
207.205.230.128
207.205.230.117
207.205.249.112
207.205.230.102
207.205.230.174
207.205.230.134
207.205.230.118
207.205.249.117
207.205.230.126
207.205.230.112
207.205.230.169
207.205.230.155
207.205.249.101

Map of the Internet, The Opte Project, www.opte.org

What do we do there?

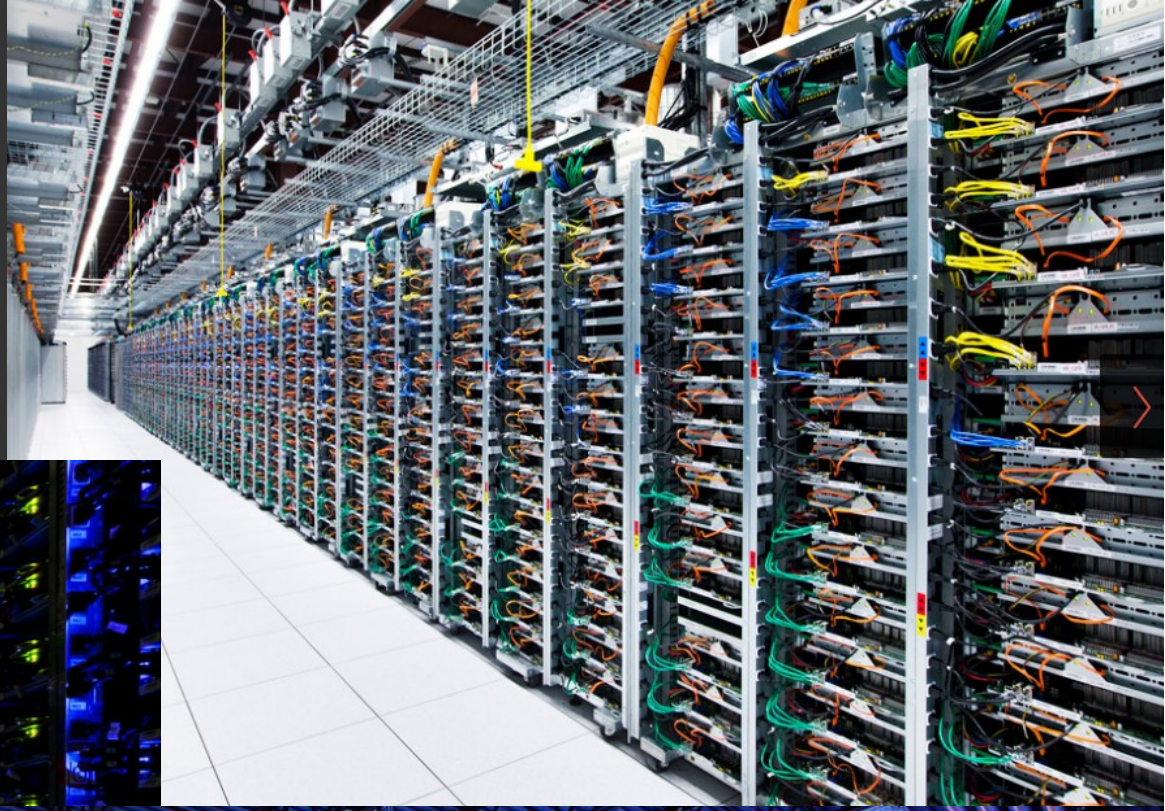
- read & write
- information
- places and maps
- emails
- speaking (IM or VOIP)
- watching pictures
- connect to old friends
- regional, national and international news
- news of people, things & gadgets
- watch the news online
- entertaining
- listen to music
- listen to podcasts
- education
- buying things or services (e.g. travel)
- online banking
- how-tos and do-it-yourself info
- looking for a job or a place to live

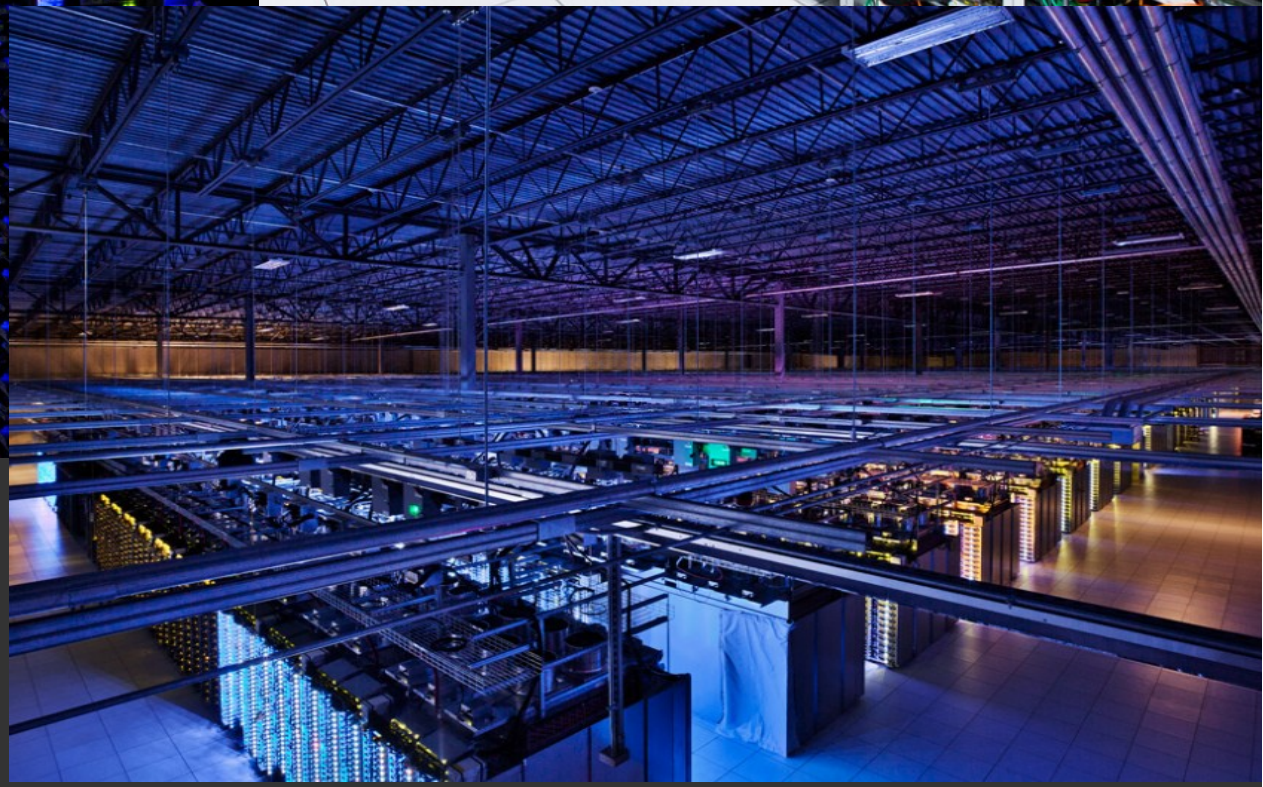
Was benutzen wir?

Services

Meist webbasiert,

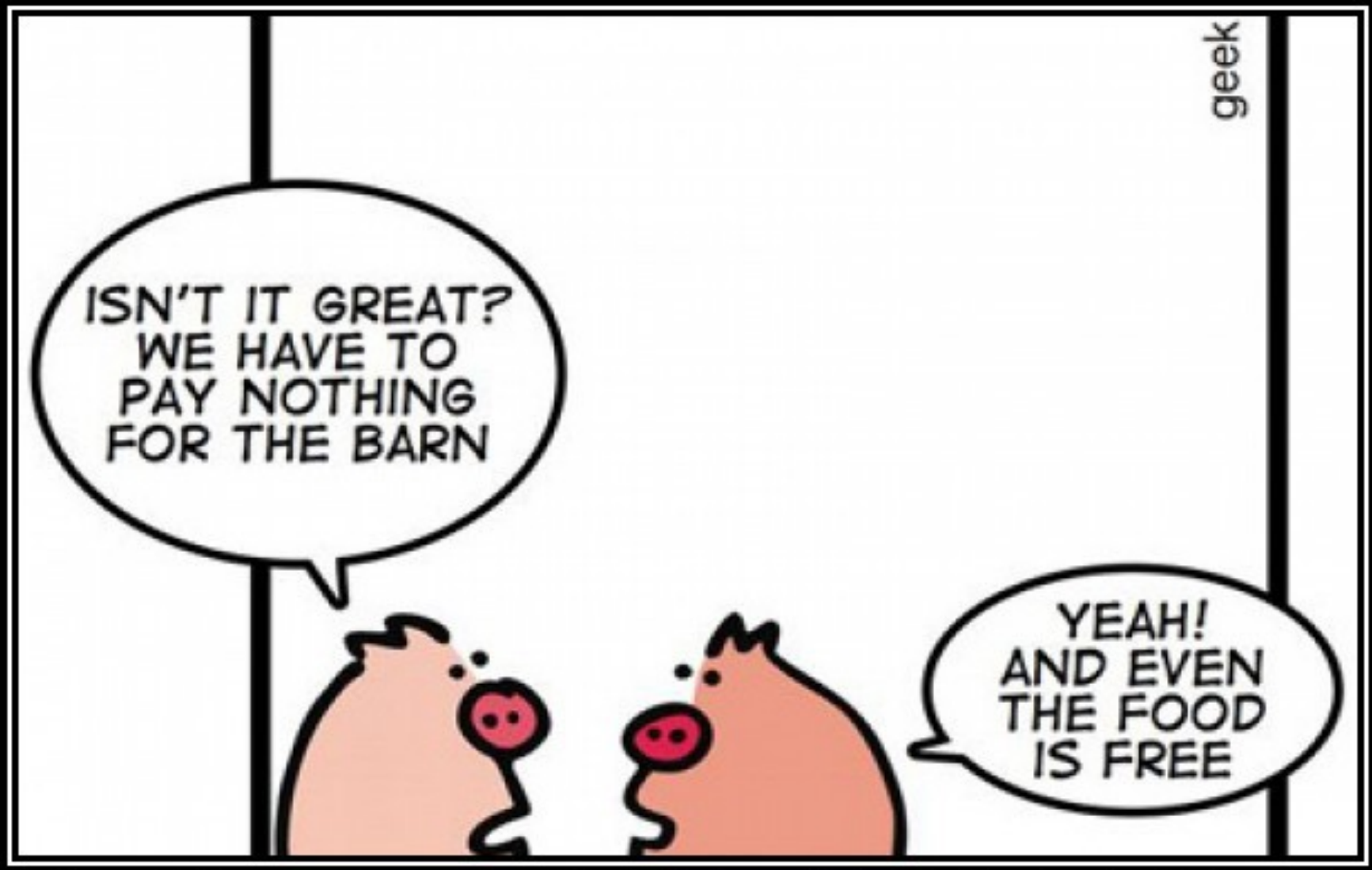
also Webseiten






Google


OIL MAKE UP TANK 150L



FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.


MONEY MONEY MONEY
Source: commons.wikimedia.org

Source: http://www.flickr.com/photos/beglen/157949514/in/photostream/

Source: http://pixabay.com/en/window-shutter-red-wood-curtain-177320/

Source: commons.wikimedia.org

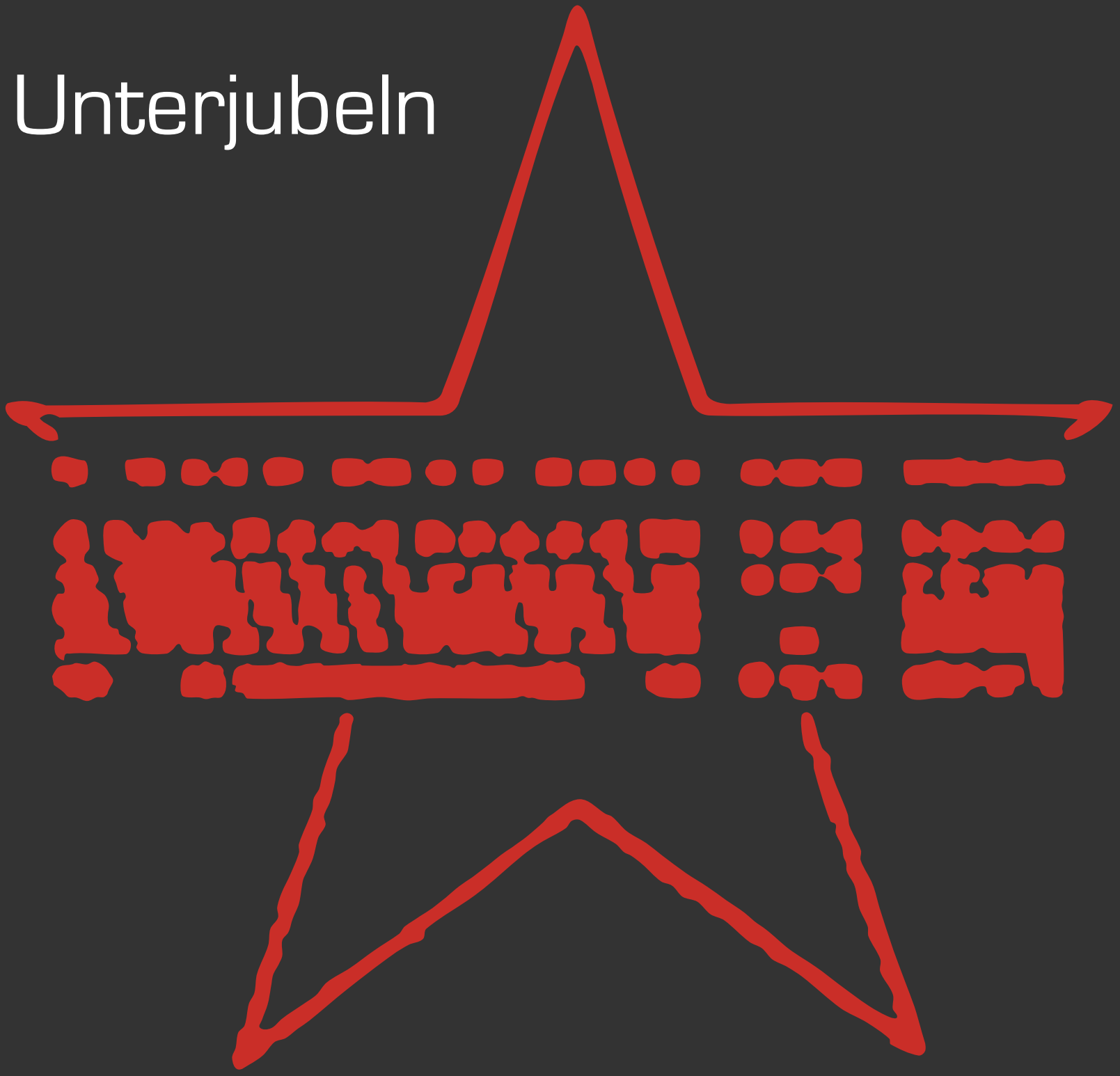

Source: commons.wikimedia.org


Source: commons.wikimedia.org

Source: http://www.flickr.com/photos/home_of_dreams/2784385818/lightbox/

Akzeptanz

Unterjubeln

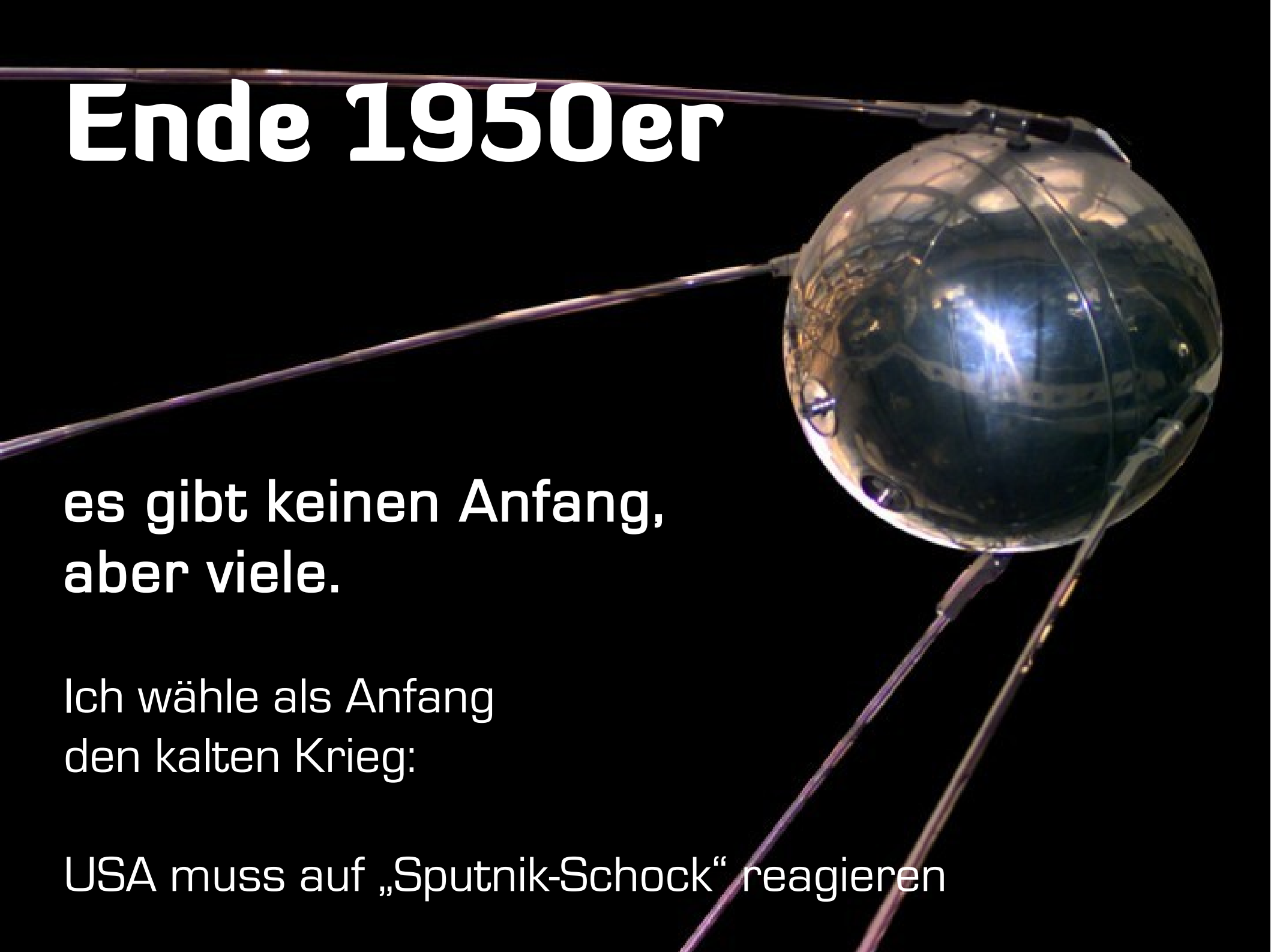


Was ist das Internet?

Wo kommt es her?

Wo geht es hin?

Ende 1950er



**es gibt keinen Anfang,
aber viele.**

Ich wähle als Anfang
den kalten Krieg:

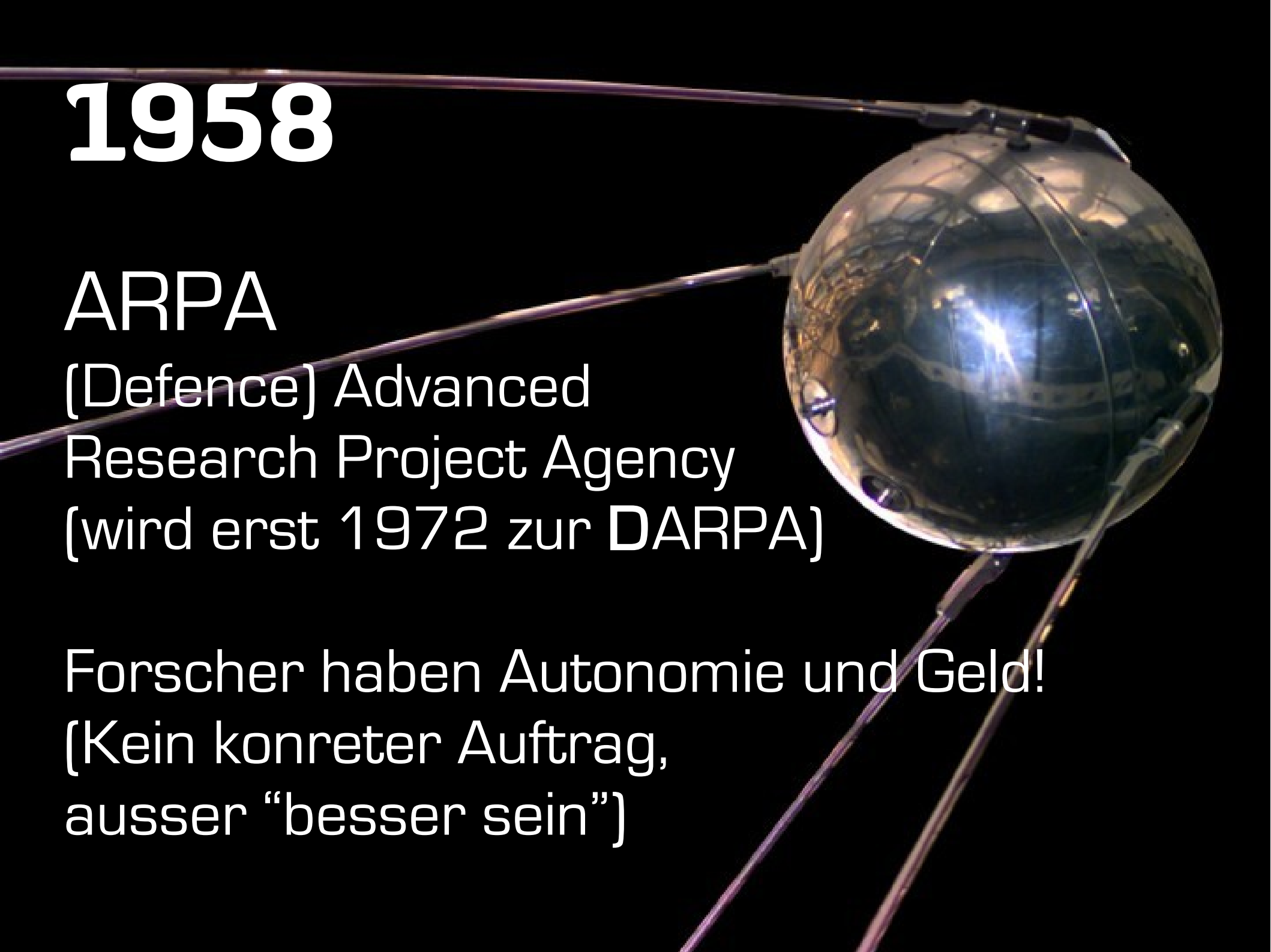
USA muss auf „Sputnik-Schock“ reagieren

1957

Sputnik

Beginn in Mißtrauen und Neid

1958



ARPA

(Defence) Advanced
Research Project Agency
(wird erst 1972 zur **D**ARPA)

Forscher haben Autonomie und Geld!
(Kein konreter Auftrag,
ausser “besser sein”)

1961

Leonard Kleinrock

Information Flow in Large Communication Nets

Theoretische Machbarkeit von paketweiser Kommunikation

C. INFORMATION FLOW IN LARGE COMMUNICATION NETS

The purpose of this investigation is to consider the problems associated with information flow in large communication nets. The nets considered consist of nodes that receive, sort, store, and transmit messages entering and leaving by way of the links (one-way channels that connect the nodes together).

Very little effort has been devoted to these problems in published works, although there is a clear practical need for an understanding of these nets. Jackson (1) has considered a class of related problems dealing with a system of departments in which messages travel between the departments according to a probability measure assigned to each link (including sources and sinks). His results show that it is possible to break the system down into independent elementary departments.

Packet switching?

1962

L.C.R. Licklider
Reihe von Memos:

Konzept eines "galaktischen Netzwerks":
viele miteinander verbundene Computer

Time-sharing existiert bereits
(Mehrbenutzersystem für Grossrechenanlagen)

1967

Konferenz, die RAND, NPL und ARPA Leute zusammenbringt

alle arbeiteten, ohne es zu wissen, an der

(prinzipiell) gleichen Idee...

1969

- Ersten vier Computer werden verbunden.
- Es werden immer mehr Rechner dem Netz hinzugefügt.
- Request for Comments (RFC) entstehen.
- **Erfinder sind Entwickler und Anwender.**
- **Forschungsgegenstand ist Publikationsmedium.**

Exkurs: Request for Comments

(RFC)

(Deutsch: Bitte um Kommentare)

Technische und organisatorische Dokumente werden zur Diskussion gestellt

Behalten diesen Namen, auch wenn sie sich zum Standart entwickelt haben

Heute: an die 8000 RFCs

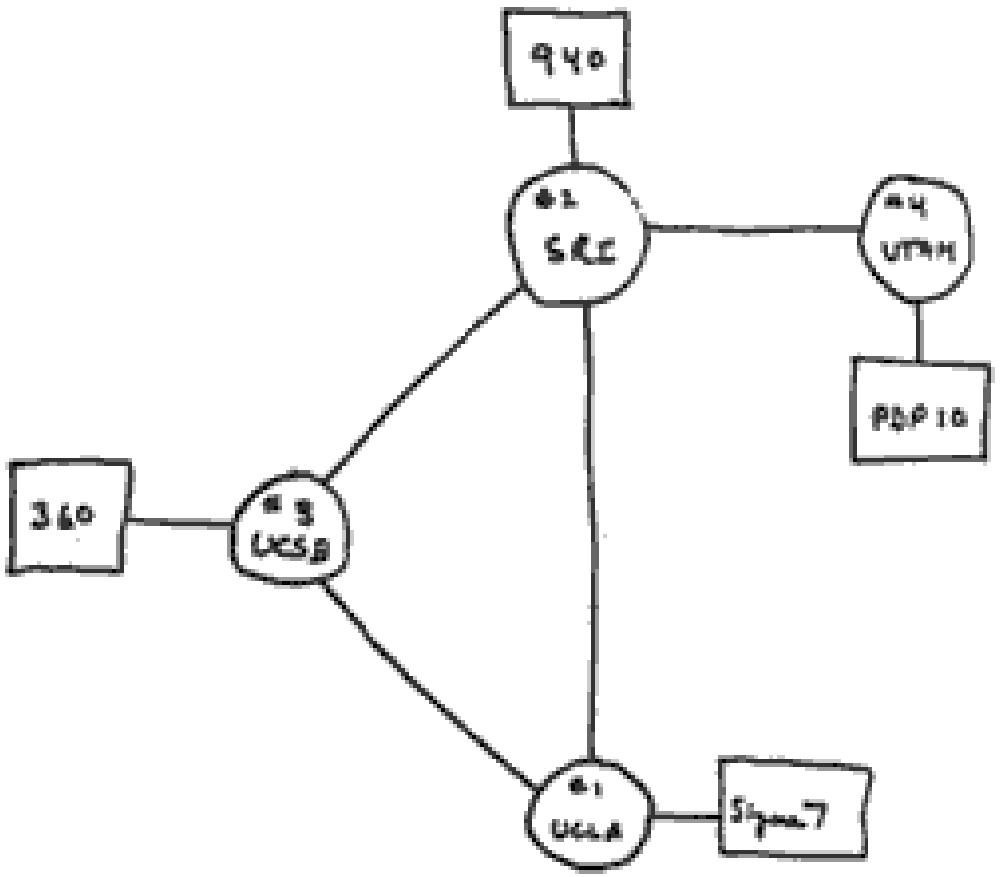
Exkurs: RFCs: Beispiele

* RFC 959 (FTP)
* RFC 1035 (DNS)
* RFC 1036 (Usenet)
* RFC 1166 (IP-Adresse)
* RFC 1436 (Gopher)
* RFC 1459 (IRC)

* RFC 1087 (Ethics and the Internet)
* RFC 2223 (Instructions to write RFC)

1969

4 Computer werden verbunden



THE ARPA NETWORK

DEC 1969

4 NODES

(Courtesy of Alex McKenzie)

The ARPANET in December 1969

1970

Network Control Protokoll ist fertig (NCP).

Anwendungen können entwickelt werden:

Telnet (Computer werden verbunden)
FTP (Information wird verbunden)
eMail (Menschen werden verbunden)

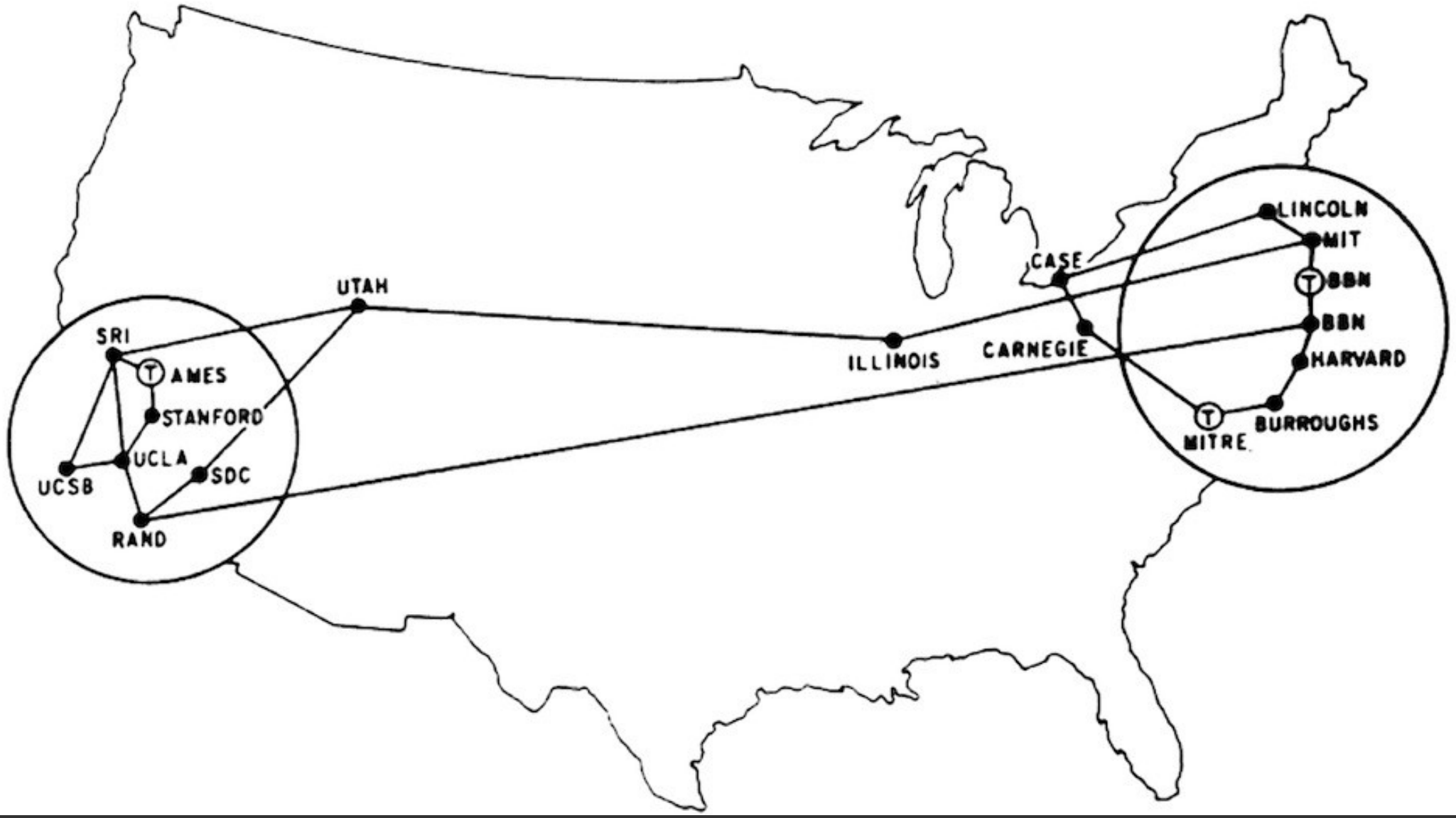
1973/74

Arpanet-Nutzer: über 2000
eMail: 75% der Ausnutzung

Immer mehr lokale Netze schliessen
sich ans "Netz der Netze" an

NCP erweist sich als untauglich
weil keine Prüfung.

Vint Cerf und Bob Kahn machen ein neues:
Transmission Control Protokoll (TCP)
⇒ wird 1978 noch in TCP/IP gesplittet.



Das Netz der Netze

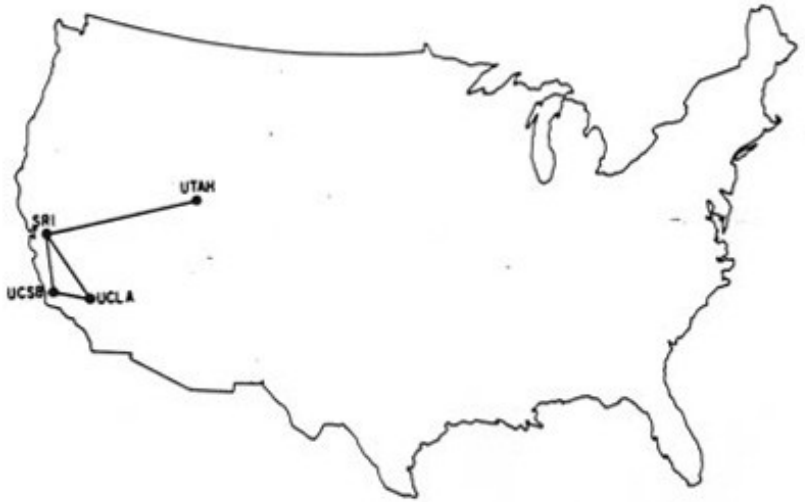


Figure 5: The ARPANET in December 1969

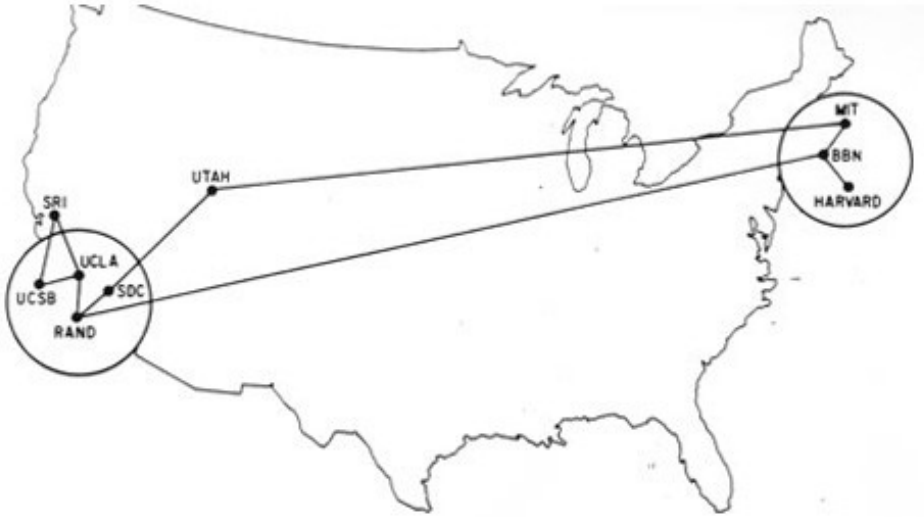
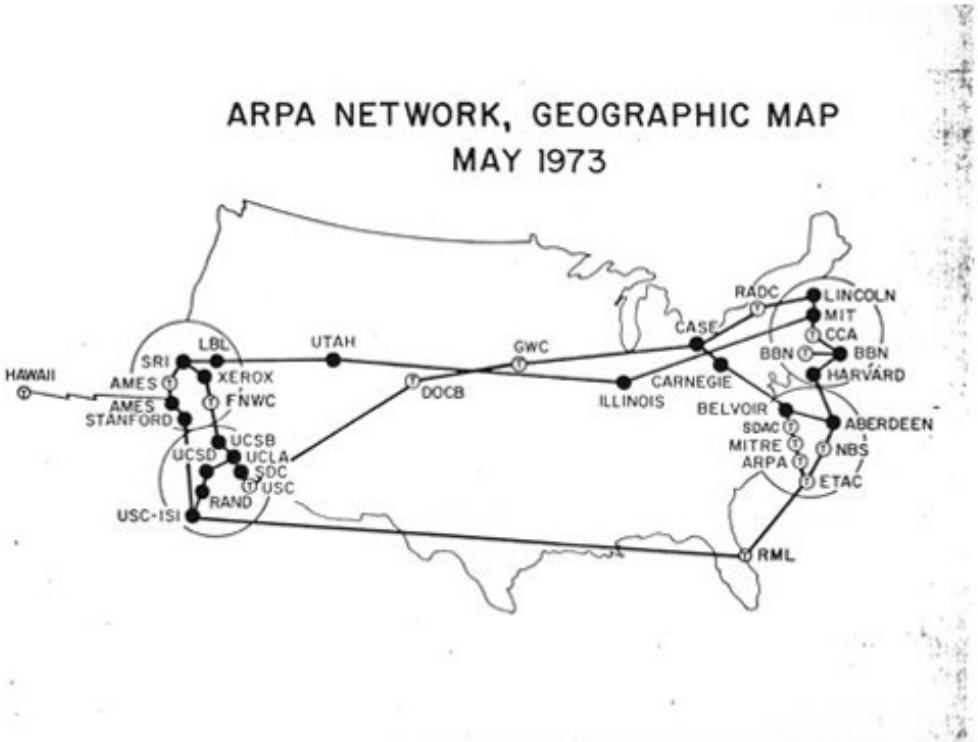
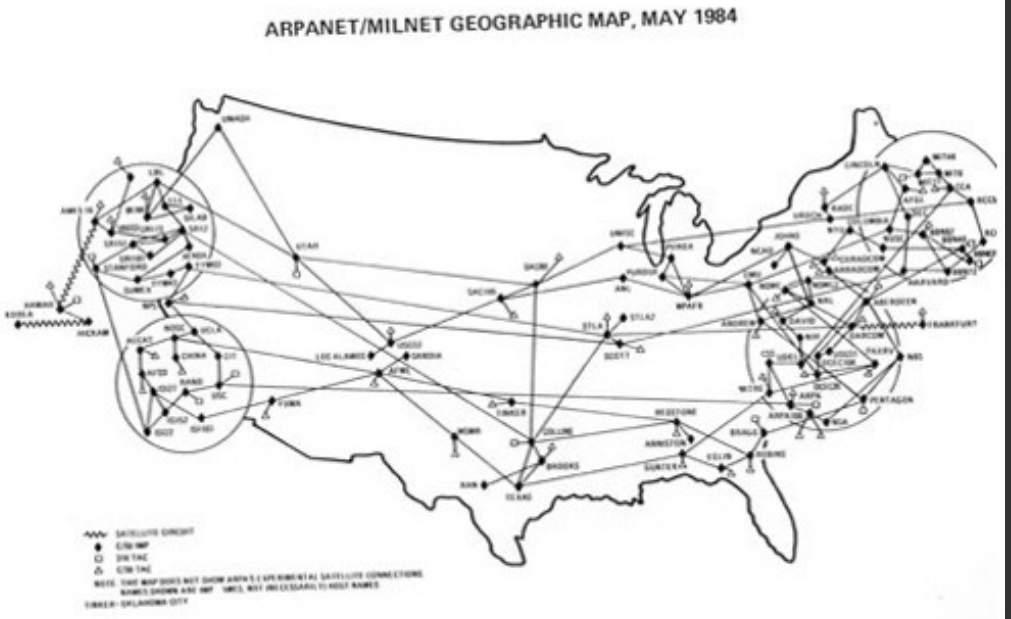


Figure 6: June 1970





1973/74

große Computerhersteller versuchen
durch die Einführung eigener Netze
Marktanteile zu sichern.

Aber: ARPANET setzt sich durch und schafft damit
freien Zugang für PCs aller Hersteller

Sie versuchens immer wieder...

1979: British Postel Service launched **Prestel**, 90,000 users
1982: France, **Minitel**: online banking, travel reservations 26,000 different services to about 25 million people.
1986: South Africa, **Beltel**

Also: Canada, Sweden, Spain, Belgium, Ireland, Japan

⇒ Internet im Internet,
aber geschlossene Netzwerke

1975

Verteilerlisten und Diskussionsgruppen entstehen.

SF-Lovers: erste nicht-technische Liste.

Wird beinahe verboten, weil keine Forschung.

Aber: Liste wird als "Pilotversuch" erlaubt.

(Herausforderung für die Techniker)

“Plapperraum” geschaffen

Raum angeeignet.

1977

Unix-to-Unix Copy (UUCP) wird mit dem Betriebssystem UNIX vertrieben
⇒ einfache Möglichkeit, Daten zu kopieren und mit anderen zu teilen.

⇒ Grundstein für "Freie Software Bewegung"

(UNIX gibts schon seit 1974 an Universitäten, mit Quellcode und Erlaubnis, diesen zu verändern)

1979

USENET und MAILBOXEN
„ARPANET des kleinen Mannes“

beinah unbeschränkter, öffentlicher Raum;
jeder kann lesen und schreiben.

Abgesehen von tech. Eingrenzungen
reguliert es sich selbst durch seine Teilhaber.

MUDs (Multi User Dungeons)
textbasierte Online Rollenspiele

1979

¯_(ツ)_/¯

Erste belegte Nachricht, in der

-) vorgeschlagen wird:

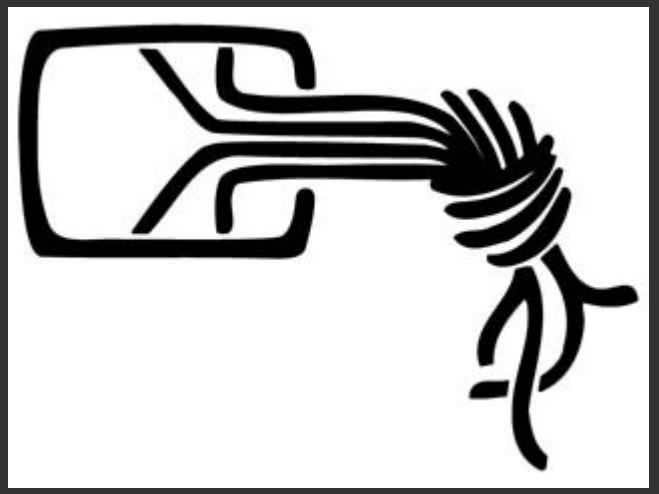
Ironie
(tongue-in-cheek)

Später:

:) :-)

:-(:(

(^_^)



1981

Chaos Computer Club wird gegründet.

Zuerst offene Verbindung,

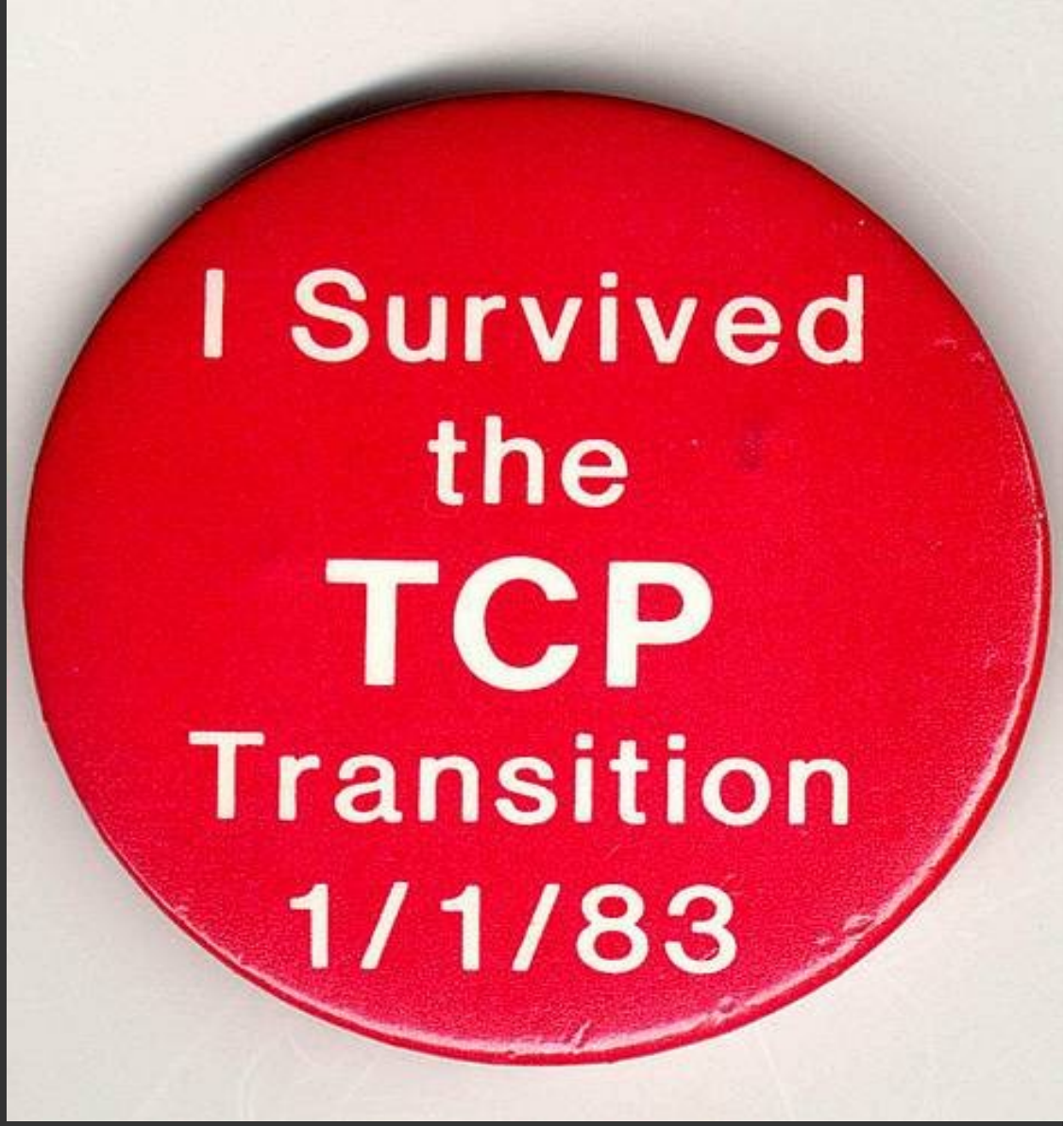
seit 1986 eingetragener Verein

(aber trotzdem sehr offen in seinen Strukturen)

1983

Übergang vom NCP-Protokoll zum TCP/IP-Protokoll
alle Hosts müssen gleichzeitig umwandeln!

1983: 500 Hosts
1984: 1000 Hosts
1987: 10.000 Hosts
1989: 100.000 Hosts



ARPANET wird geteilt in militärisches MILNET und restliches ARPA-INTERNET. Weit über die Hälfte der Knoten gingen an das MILNET.

1984

Domain Namen System (DNS)

⇒ Schritt Richtung Anwenderfreundlichkeit.

William Gibson erwähnt in
Neuromancer den Begriff *Cyberspace*

CYBER CYBER CYBER CY
CYBER CYBER CYBER CY

1986

NSFNET (National Science Foundation NET)

⇒ Backbone des neuen Internets

(bisher war dies das ARPANET).

1988

Internet Relay Chat (IRC)

(dezentrales Chatsystem, in dem jeder eigene Räume eröffnen kann)

wird von einem finnischen Studenten entwickelt.

IRC wird bis heute rege genutzt.

1990

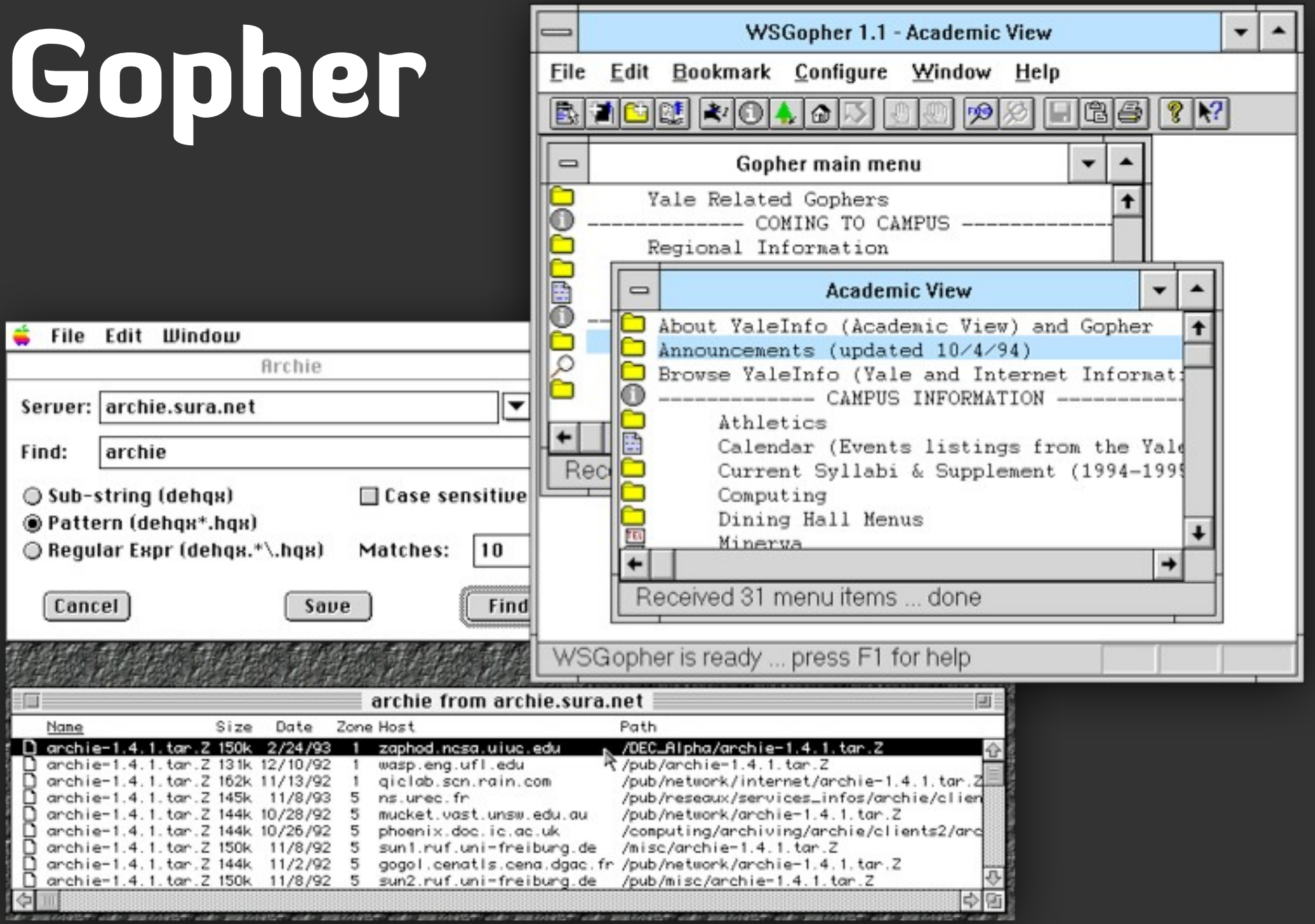
ARPANET wird abgeschaltet

für seine Nutzer ändert sich
dank des NSFNETs kaum etwas.

Gopher entsteht
(ein eigenständiges System, das man sich
in etwa so vorstellen kann wie das Web)

Gründung Electronic Frontier Foundation (EFF)

Gopher


WSGopher 1.1 - Academic View
File Edit Bookmark Configure Window Help
Gopher main menu
Yale Related Gophers
COMING TO CAMPUS
Regional Information
Academic View
About YaleInfo (Academic View) and Gopher
Announcements (updated 10/4/94)
Browse YaleInfo (Yale and Internet Informat
CAMPUS INFORMATION
Athletics
Calendar (Events listings from the Yale
Current Syllabi & Supplement (1994-199
Computing
Dining Hall Menus
Minerva
Received 31 menu items ... done
WSGopher is ready ... press F1 for help
File Edit Window
Archie
Server: archie.sura.net
Find: archie
Sub-string (dehqx)
Case sensitive
Pattern (dehqx*.hqx)
Regular Expr (dehqx.*\.hqx)
Matches: 10
Cancel
Save
Find
archie from archie.sura.net
Name Size Date Zone Host Path
archie-1.4.1.tar.Z 150k 2/24/93 1 zaphod.ncsa.uiuc.edu /DEC_Alpha/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 131k 12/10/92 1 wasp.eng.ufl.edu /pub/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 162k 11/13/92 1 qiclab.scn.rain.com /pub/network/internet/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 145k 11/8/93 5 ns.urec.fr /pub/reseaux/services_infos/archie/clien
archie-1.4.1.tar.Z 144k 10/28/92 5 mucket.vast.unsw.edu.au /pub/network/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 144k 10/26/92 5 phoenix.doc.ic.ac.uk /computing/archiving/archie/clients2/arc
archie-1.4.1.tar.Z 150k 11/8/92 5 sun1.ruf.uni-freiburg.de /misc/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 144k 11/2/92 5 gogol.cenatls.cena.dgac.fr /pub/network/archie-1.4.1.tar.Z
archie-1.4.1.tar.Z 150k 11/8/92 5 sun2.ruf.uni-freiburg.de /pub/misc/archie-1.4.1.tar.Z

1990

Tim Berners-Lee schreibt ein Programm:
"WorldWideWeb"

„Ich kam zufällig zur rechten Zeit und mit den passenden Interessen und Neigungen, nachdem der Hypertext und das Internet zu ihre Volljährigkeit erreicht hatten. Die einzige Aufgabe, die mir blieb, war es, die beiden miteinander zu verheiraten.“

Es entstehen Browser – keine Editoren.
Meist nur passive Teilhabe.

1993

Langsam nimmt die Medien- und Business-Welt Notiz vom Internet.

Gopher macht den Fehler, Lizenzgebühren für die Nutzung ihres Dienstes zu verlangen.

Im April stimmt der Arbeitgeber von Berners-Lee (CERN) der unbeschränkten und kostenlosen Nutzung des Webs zu.

1994

Am 14. Dezember ist die erste Konferenz des World Wide Web Consortiums (W3C)

„neutrale Versammlung derjenigen, denen das Web wichtig ist, mit der Mission, die Ausschöpfung des vollen Potentials das Webs zu ermöglichen.“

„Gremium zur Standardisierung der World Wide Web betreffender Techniken“ und deren Weiterentwicklung.

(Nutzen nur patentfreie Technologien)

1996

A Declaration of the Independence of Cyberspace

https://projects.eff.org/~barlow/Declaration-Final.html

John Perry Barlow (EFF)

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. [...]"

1998

Internet Corporation for Assigned Names and Numbers (ICANN)

⇒ wird von einem Zusammenschluss verschiedener Interessenverbände (Wirtschaft, Technik, Wissenschaft und Nutzer) gegründet.

1998-2000

Das Internet, bzw das Web wird bekannter.
Viele neue Unternehmen - gehen an die Börse.

Gegen Ende des Jahrhunderts werden durch steigende Nachfrage viele dieser Unternehmen und Geschäftsideen überbewertet.

Im März 2000 platzt die sogenannte Dotcom-Blase und resultiert in einem Börsencrash.

2001

Wikipedia entsteht

eine „von freiwilligen Autoren verfasste,
mehrsprachige, freie Online-Enzyklopädie“

Freifunk startet (mehr dazu später)

(um die gleiche Zeit werden Blogs “hip”)

2004

Ende 2004 wird der Begriff Web 2.0 zum ersten mal offiziell verwendet.

Es gibt (immer noch!) keine klare Definition.

(zunächst Marketing Begriff, wird aber angenommen)

Zurück zur ursprünglichen Idee des many-to-many

Aber: zentrale Währung sind Daten!

2005

NSFNET-Internet-Backbone wird stillgelegt

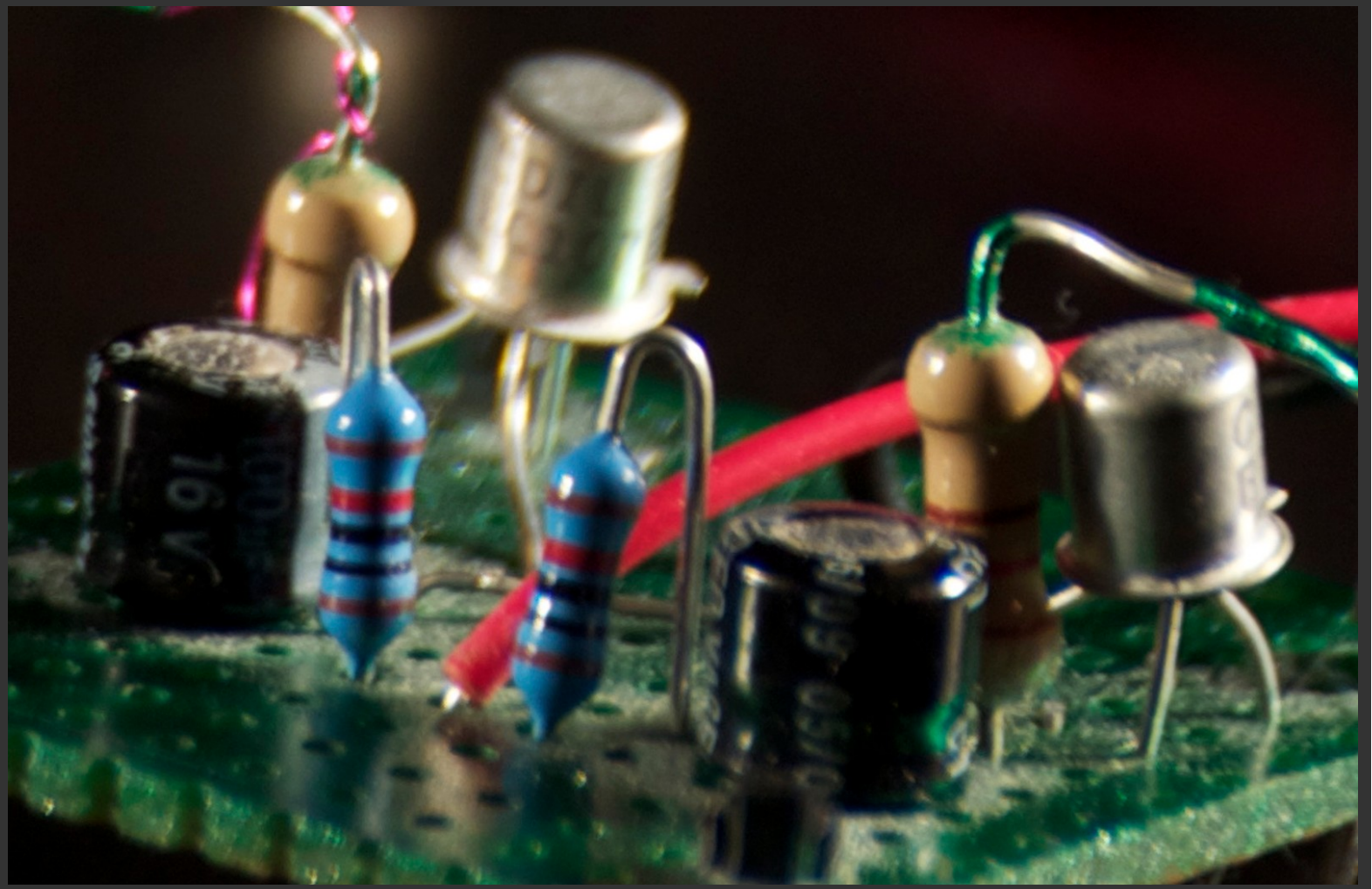
Nun besteht das Internet aus vielen privaten Netzwerken und kommerziellen Internet Service Providern (ISP).

Netzneutralität!

2006

Facebook

Twitter



2007

Vorratsdatenspeicherung

im November beschlossen,

(März 2010 vom Bundesverfassungsgericht

für nichtig erklärt, aber bleibt ZOMBIE!)

2008

Wikileaks wird bekannt

Nicht nur durch Vorratsdatenspeicherung

(aber auch!) verändert sich vieles

⇒ Notwendigkeit einer Zwischeninstanz

2009

#zensursula

Trotz “Tabuthema”

134.000 Unterschriften bei Petition

Netz und Infrastruktur sind und bleiben

unverstanden (nicht nur) bei den

Gesetzgebenden

2010

Spamquote bei E-Mails liegt bei 95%

Beim LRZ (wissenschaftliches Hochleistungsrechenzentrum in München)

99,5%

2011

Die letzten IPv4 Adressen wurden vergeben

IPv4: 4.294.967.296 Adressen
IPv6: 340.282.366.920.938.463.463.374.
607.431.768.211.456 Adressen

(Auf jedem mm^2 der Erde
665.570.793.348.866.944
Adressen)

2013

Snowden

Sie machens wirklich.
Obwohl wir doch gar nichts zu verbergen haben.

[redacted] nothing [redacted]
[redacted] to [redacted]
[redacted] hide [redacted]

Wie weiter?

Verschlüsselung / Cryptography

Was ist Crypto?

Mathematische Methode um
Daten nur lesbar zu machen für

Sender
Empfänger

⇒ Ende-zu-Ende Verschlüsselung

Basic Principles

Confidentiality

(no one else can read it)

Integrity

(no one else can modify)

Authentication

(message is from the one person)

Be Aware!

you are never “safe”
technology can fail.

It can fail any time.
Without you even noticing.

Never Forget!

encrypt (or encode)
verschlüsseln (oder enkodieren)

⇒ Code

or Key

Simple encoding/key:

Hello

⋮

⋮

olleH

Software hilft:

Hello

⋮

⋮

hQEMAy4io41ThT7gAQgAqF7ljcgd

Private Means...

...nur du & ich haben den key
niemand sonst kann zuhören

⋮

uSMWsh3zbWke8DUmY+Lf9Ssy2waJkE+gaJKhxplD6CWfL96vgXn3N/bBVg2+SCmt
UV/btwupjojluio1cLS0X85glj85sfeALHZGDzRTe7kuMXSqY9A+ZEpYIGybGkLk
8EjFZOqgDNRZRVe2mXpu7EOEwXEuIl2cANk5iXaVanAHGSMubUEzwkZWxvfHdPSZ
DWK9AYBRyIr62k8W7/rvpI8T8RtuinPbVWl5sLe7/x0smFvVfYj0Cy+UakOLgN08
4yghqyWWY7Hzc1Xq+UQrVib8CVnk5h/WQotuOshBmdLpAWMYkbNV3eJMxQ4xqx0u

Aber...

...jede/r weiss dass wir zwei miteinander sprechen

:

:

metadata bleibt Klartext:
Zeit, Ort, IP, System, Sprachen, Schriften, Fenstergrößen, etc.

(alles ausser des Hauptteils Deiner email/text)

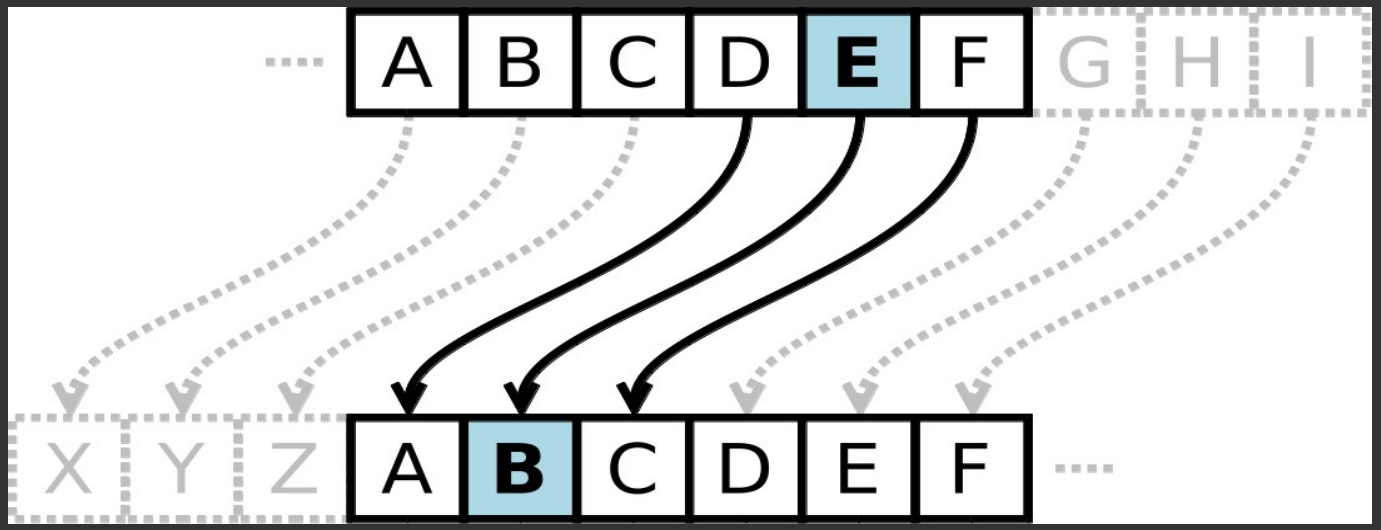
E-Mail

GPG

Asymmetric Encryption

Symmetric Encryption

Wie vor 2000 Jahren bei Julius Caesar



Hello

⋮

Ebiil

key/code == “alphabet: left-shift-3”

Both sides have to know key/code=> symmetric

Asymmetric Encryption: Keys

Oftmals auch: “public-key-encryption”

Jede/r hat ein key-paar:

public key

available for everyone

secret key

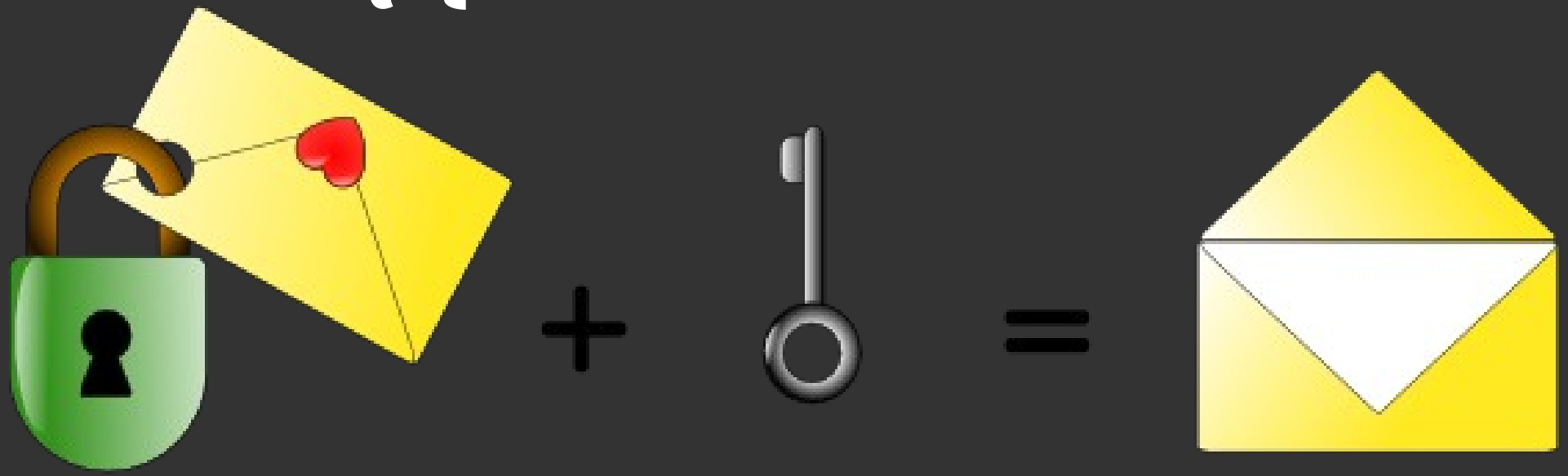
kept as a secret

Asymmetric Encryption: En-crypt

Bob uses the open lock / public key from Alice to lock/encrypt the message.

Once closed, he is not able to open it any more.

Asymmetric Encryption: De-crypt



Alice uses her secret key to unlock/ decrypt the message from Bob.

Alice is the only one able to open this message.

Asymmetric Encryption: Sign

But, the analogy will not fit for the next layer of understanding. Usually an encrypted text is **encrypted with the recipients public key** and **signed with your private key**.

Alice	Bob
private	public
X	
public	private

Asymmetric Encryption: Sign

This works like a seal of wax on ancient letters: The king only has the original stamp, but the normal person can prove by the picture of it.

Alice	Bob
private	public
public	private

E-Mail

transferred as plain text

content
metadata
whole route
everything

Service Providers? => TRUST!

- Use a friends mail server
- Pay for the service
- Combine the above
- Use mail server from a non-profit organization (and donate if possible)
- Use a mail server from a profit organization that earns money with services

Content in an Envelope?

1. Mail App + (add-on)

   (z.B.:mozilla.org/thunderbird + enigmail)

2. Install GnuPG (gnupg.org)

3. Generate key-pair, publish public key

Use!

(Alternative: p≡p, see pep-project.org)

Remember...

...everyone knows that the two of us are talking to each other

⋮

⋮

metadata stays plain text, like time, place, IP, system, etc.

(everything besides the main body of your email/text)

(sometimes you might wanna add anonymity)

Status quo

The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together

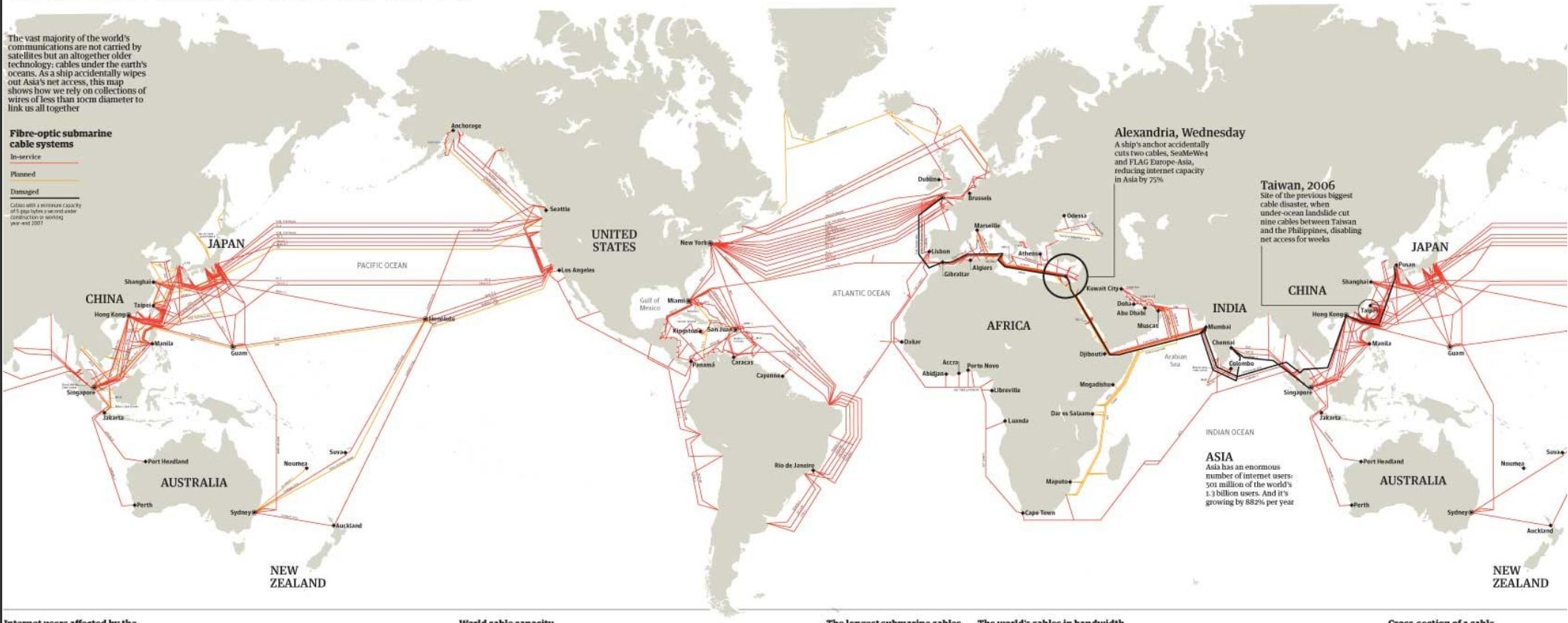
Fibre-optic submarine cable systems

In-service

Planned

Damaged

Cables with a minimum capacity of 5 giga-bytes a second under construction or working year-end 2007



Alexandria, Wednesday

A ship's anchor accidentally cuts two cables, SeaMeWe4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

Taiwan, 2006

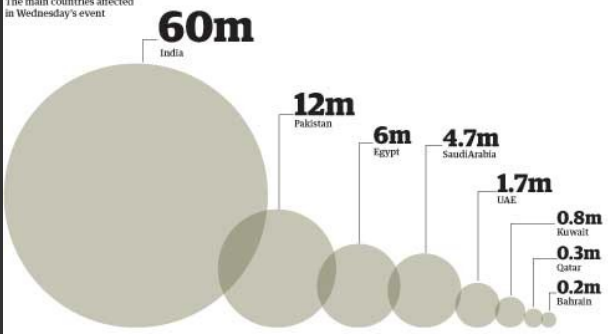
Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA

Asia has an enormous number of internet users: 501 million of the world's 1.3 billion users. And it's growing by 882% per year

Internet users affected by the Alexandria accident

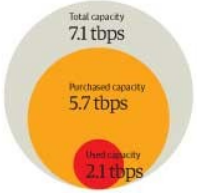
The main countries affected in Wednesday's event



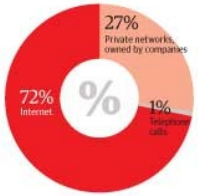
World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terabytes a second



What makes up "used capacity"?



The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

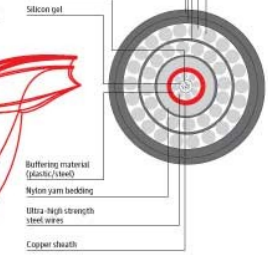
SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

The world's cables in bandwidth

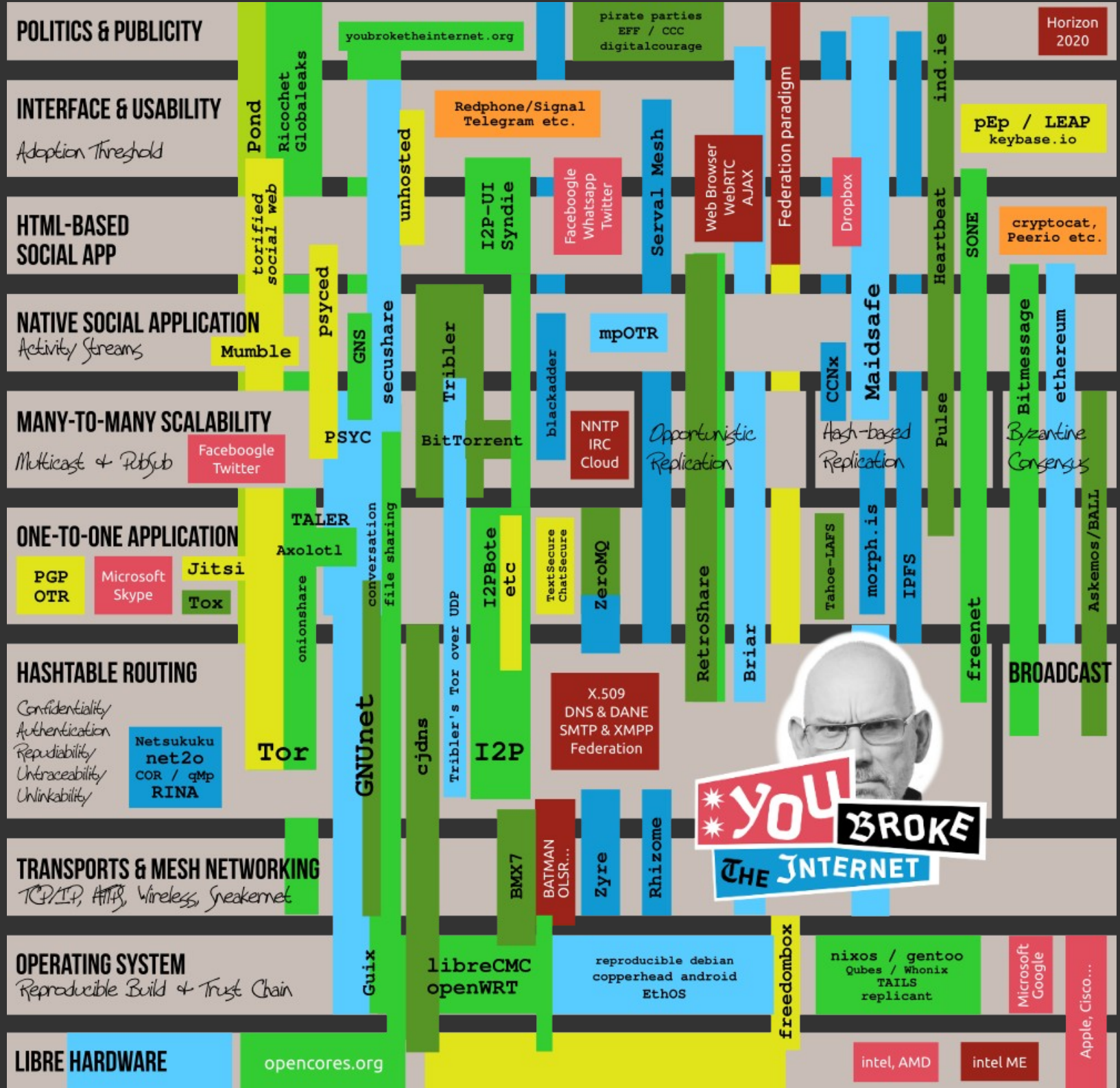
The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

Cross-section of a cable

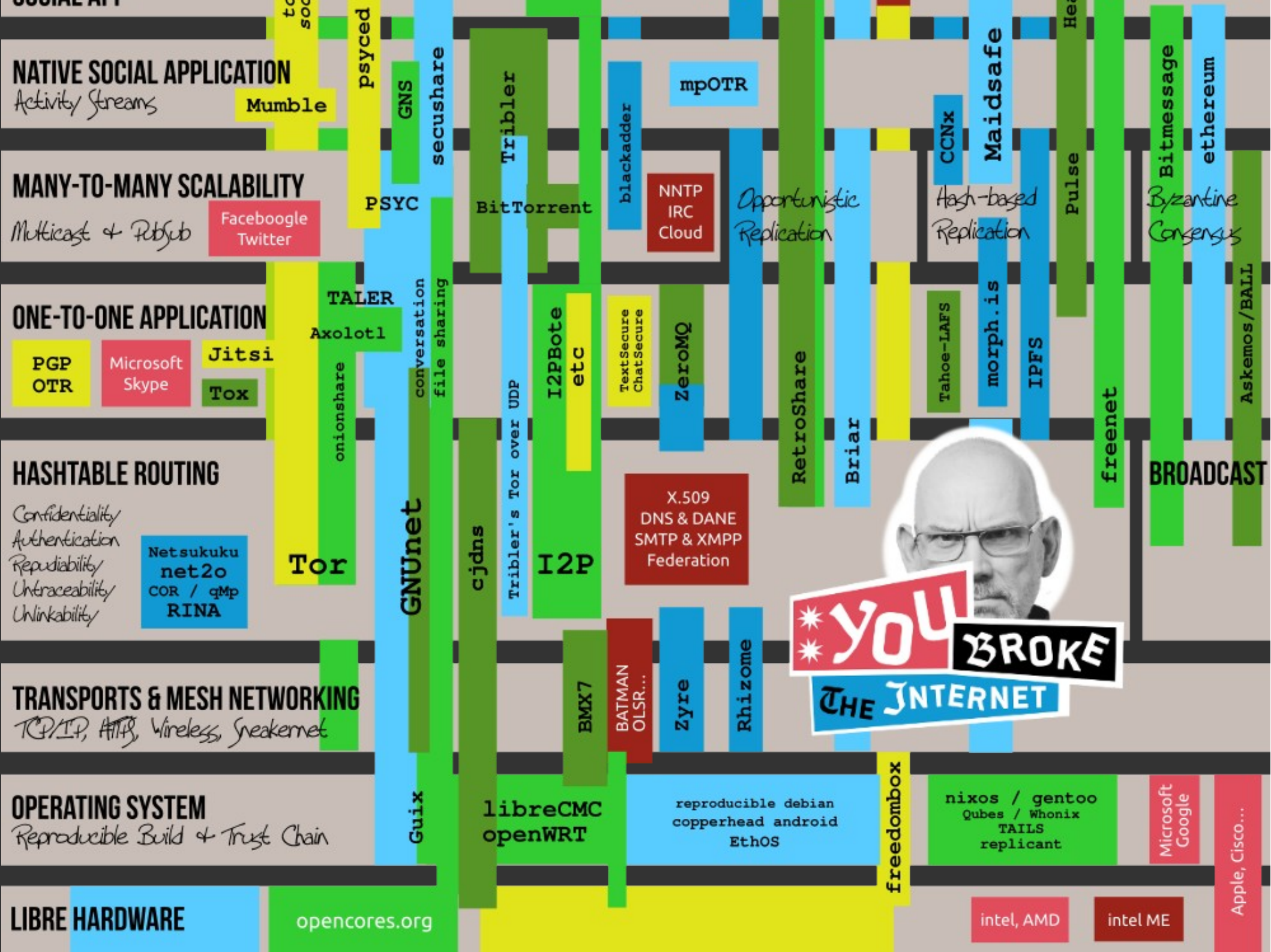
Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used



SOURCE: TELEGEOGRAPHY.COM SUBMARINE CABLE MAP 2008, INTERNET STATISTICS FROM INTERNETWORLDSTATS.COM



http://youbroketheinternet.org/map


NATIVE SOCIAL APPLICATION
Activity Streams
Mumble
psyced
GNS
secushare
Tribler
mpOTR
blackadder
Maidsafe
Bitmessage
ethereum
MANY-TO-MANY SCALABILITY
Multicast + PubSub
Faceboogle
Twitter
PSYC
BitTorrent
NNTP
IRC
Cloud
Opportunistic
Replication
CCNx
Hash-based
Replication
Pulse
Byzantine
Consensus
ONE-TO-ONE APPLICATION
PGP
OTR
Microsoft
Skype
Jitsi
Tox
TALER
Axolotl
onionshare
conversation
file sharing
I2PBote
etc
TextSecure
ChatSecure
ZeroMQ
Tahoe-LAFS
morph.is
IPFS
Askemos/BALL
HASHTABLE ROUTING
Confidentiality
Authentication
Repudiability
Untraceability
Unlinkability
Netsukuku
net2o
COR / qMp
RINA
Tor
GNUnet
cjdns
Tribler's Tor over UDP
I2P
X.509
DNS & DANE
SMTP & XMPP
Federation
RetroShare
Briar
freenet
BROADCAST
YOU BROKE THE INTERNET
TRANSPORTS & MESH NETWORKING
TCP/IP, HTTP, Wireless, Sneakernet
BMX7
BATMAN
OLSR...
Zyre
Rhizome
OPERATING SYSTEM
Reproducible Build + Trust Chain
Guix
libreCMC
openWRT
reproducible debian
copperhead android
EthOS
freedombox
nixos / gentoo
Qubes / Whonix
TAILS
replicant
Microsoft
Google
Apple, Cisco...
LIBRE HARDWARE
opencores.org
intel, AMD
intel ME


POLITICS & PUBLICITY
youbroketheinternet.org
pirate parties
EFF / CCC
digitalcourage
Horizon 2020
INTERFACE & USABILITY
Adoption Threshold
Pond
Ricochet
Globaleaks
Redphone/Signal
Telegram etc.
pEp / LEAP
keybase.io
ind.ie
HTML-BASED SOCIAL APP
torified social web
unhosted
I2P-UI
Syndie
Faceboogle
Whatsapp
Twitter
Serval Mesh
Web Browser
WebRTC
AJAX
Federation paradigm
Dropbox
Heartbeat
SONE
cryptocat,
Peerio etc.
NATIVE SOCIAL APPLICATION
Activity Streams
Mumble
psyced
GNS
secushare
Tribler
mpOTR
blackadder
Maidsafe
Pulse
Bitmessage
ethereum
MANY-TO-MANY SCALABILITY
Multicast + PubSub
Faceboogle
Twitter
PSYC
BitTorrent
NNTP
IRC
Cloud
Opportunistic
Replication
CCNx
Hash-based
Replication
Byzantine
Consensus
ONE-TO-ONE APPLICATION
PGP
OTR
Microsoft
Skype
Jitsi
Tox
TALER
Axolotl
onionshare
conversation
file sharing
I2PBote
etc
TextSecure
ChatSecure
ZeroMQ
RetroShare
Briar
Tahoe-LAFS
morph.is
IPFS
freenet
Askemos/BALL
HASHTABLE ROUTING
Confidentiality
Authentication
Repudiability
Untraceability
Unlinkability
Netsukuku
net2o
COR / qMp
RINA
Tor
GNUnet
cjdns
Tribler's Tor over UDP
I2P
X.509
DNS & DANE
SMTP & XMPP
Federation
BROADCAST
YOU
BROKE

Wo k nnte es hingehen?

Beispielprojekte

Bürgernetze & Freifunk

FreedomBox

GNUnet

Bürgernetzverband e.V.

gemeinnütziger Verband der Bürgernetze in Deutschland

Internet für jeden nutzbar machen

(seit 1995, ehrenamtlich)

44 lokale Vereine, 25.000 Mitglieder deutschlandweit

Vor allem in Bayern, aber auch Sachsen und Thüringen

Anfangs: Zugang zum Internet schaffen

Bürgernetzverband e.V.

gemeinnütziger Verband der Bürgernetze in Deutschland

Heute: Aufklärung und Fortbildung

"Vernetzung von unten"

"Selbst ausprobieren"

"Austausch vor Ort"

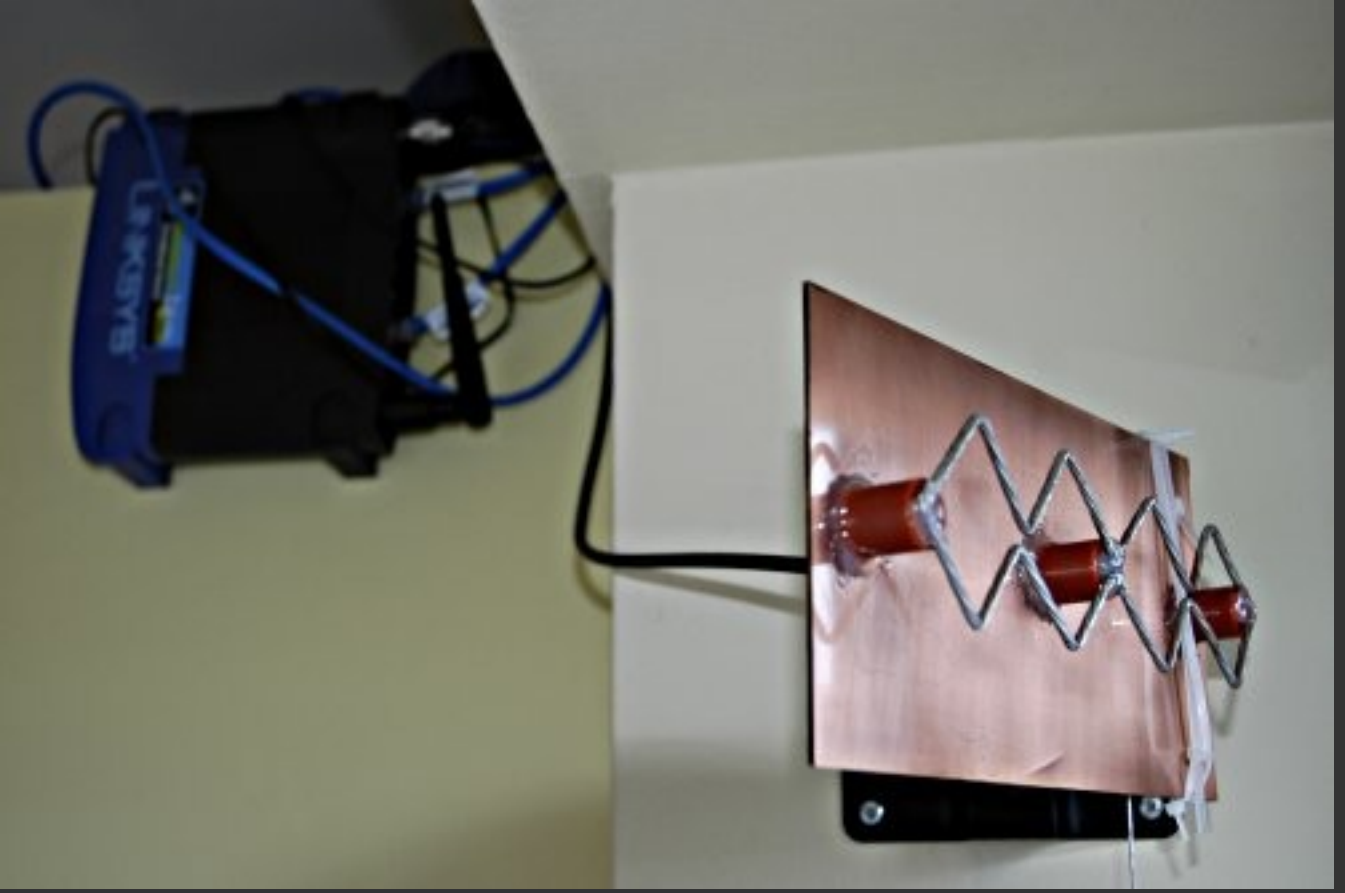
"Die Mitgestaltung des Internets durch die Bürger bedeutet schließlich auch Mitgestaltung der Demokratie in Deutschland!"

freifunk.net

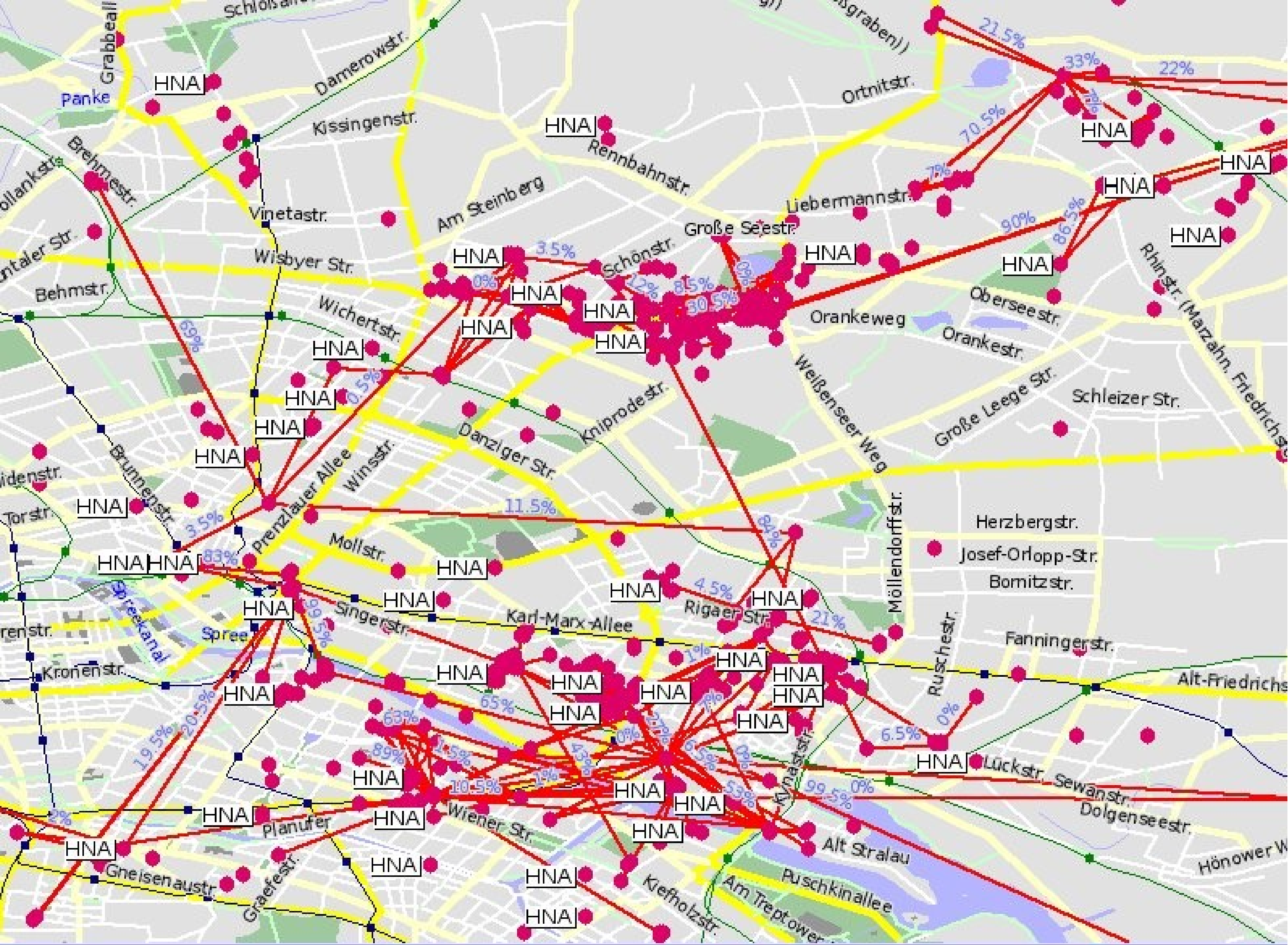
“Unsere Vision ist die Demokratisierung der Kommunikationsmedien durch freie Netzwerke”

(Seit 2000)


LINKSYS



freifunk.net



Grabbeallee
Panke
Damerowstr.
Kissingenstr.
Ortnitstr.
Rennbahnstr.
Brehmestr.
Vinetastr.
Am Steinberg
Liebermannstr.
Große Seestr.
Wisbyer Str.
Schönstr.
Behmstr.
Wichertstr.
Orankeweg
Oranke str.
Obersee str.
Weißenseer Weg
Kniprodestr.
Große Leege Str.
Schleizer Str.
Danziger Str.
Brunnenstr.
Prenzlauer Allee
Winsstr.
Mollstr.
Herzbergstr.
Josef-Orlopp-Str.
Bornitzstr.
Möllendorffstr.
Singerstr.
Karl-Marx-Allee
Rigaer Str.
Fanningerstr.
Ruschestr.
Alt-Friedrichs
Spree
Spreekanal
Kronenstr.
Lückstr.
Sewanstr.
Dolgenseestr.
Planufer
Wiener Str.
Alt Stralau
Gneisenaustr.
Graefestr.
Kiefholzstr.
Puschkinallee
Am Treptower
Hönower W
Kynaststr.
HNA
21.5%
33%
22%
70.5%
7%
90%
86.5%
3.5%
0%
12%
8.5%
30.5%
69%
0.5%
11.5%
84%
83%
99.5%
4.5%
21%
1%
65%
63%
2.7%
6.5%
53%
89%
10.5%
43%
99.5%
20.5%
19.5%
2%

FreedomBox

Kleiner, preiswerter, einfacher Computer.

Soll “Freiheit nachhause bringen”

- privacy
- control
- easy to use
- Dehierarchicali-sation

- Günstige Harware
- Leicht zu installierende und zu administrierende Software
- Existente Services sollen leicht eingebunden werden können

Vision Statement

"We live in a world where our use of the network is mediated by **organizations that often do not have our best interests at heart**. By building software that does **not rely on a central service, we can regain control and privacy**. By keeping our data in our homes, we gain useful legal protections over it. By giving back **power to the users** over their networks and machines, we are **returning the Internet to its intended peer-to-peer architecture**."

(Hervorhebungen von mir)

GNUnet

let's make a GNU one

GNUnet is...

"a **mesh routing layer** for
end-to-end encrypted networking and

a **framework for distributed applications**

designed to
**replace the old insecure
Internet protocol stack.**"

GNUnet wants to...

"....become a widely used, reliable, open, non-discriminating, egalitarian, unfettered and censorship-resistant system of free information exchange."

"....serve as a development platform for the next generation of decentralized Internet protocols."

GNUnet

"We value free speech above state secrets, law-enforcement or intellectual property."

"...an anarchistic network, where the only limitation for peers is that they must contribute enough back to the network such that their resource consumption does not have a significant impact on other users."

GNUnet

“GNUnet's primary design goals are
to protect the privacy of its users and
to guard itself against attacks or abuse.

GNUnet does not have any mechanisms to control, track or censor users. Instead, the GNUnet protocols aim to make it as hard as possible to find out what is happening on the network or to disrupt operations.”

GNUnet ausprobieren

Clone gnunet.org/git

Installationsanweisungen von der Website folgen

Sich im IRC #gnunet auf freenode helfen lassen

Auf gnunet.org/bugs reporten ;-)

Fazit 0

Wir sollten das Netz selbst wieder in die Hand nehmen. In all seinen Facetten und Layern.

(anders kommen wir da eh nicht mehr raus)

Ziele von verl sslichen Infrastrukturen

unerlässlich für...

... Zivilgesellschaften

... das Funktionieren von Demokratie und Staaten

... die Teilhabe am gesellschaftlichen, kulturellen und politischen Leben

... eine vernetzte Wirtschaftswelt

Stabile, zivile Infrastruktur

verlässlich, verfügbar

integer, robust

dezentral

(wirtschaftlich motivierte Konzentration rückgängig machen)

quelloffen

(gesamtes Design in Free Software)

heterogen

(keine Monokulturen, sowohl in Hard- und Software,
als auch bei den physikalischen Medien (Verkabelung, Funk))

Ausserdem: Breit gestreutes Wissen über IT (-Security)

=> Nicht kriminalisieren, fördern!

Ziel gemeinsamer Anstrengungen
sollte die Verlässlichkeit globaler, öffentlicher
Kommunikationsstrukturen und die Immunität
gegenüber jedweden Angriffen sein.

by Design.

Fazit I

Missonier' mal!

Free Software,
aber auch Privacy,
und warum...

Fazit II

Bau' mal!

Free Software, Crypto und vor allem:
Neue Internetprotokolle und
Anwendungen dafür!

(Auch: Hackspaces & Events!)

Fazit III

“Mögen hätt' ich schon wollen, aber dürfen hab ich mich nicht getraut!”

(Karl Valentin)

k thx bye **sva**

GNUnet must...

...be implemented as free software.
...only disclose the minimal amount of information necessary.
...be decentralised and survive Byzantine failures in any position in the network.
...make it explicit to the user which entities must be trustworthy when establishing secured communications.
...use compartmentalization to protect sensitive information.
...be open and permit new peers to join.
...be self-organizing and not depend on administrators.
...support a diverse range of applications and devices.
...architecture must be cost effective.
...provide incentives for peers to contribute more resources than they consume.