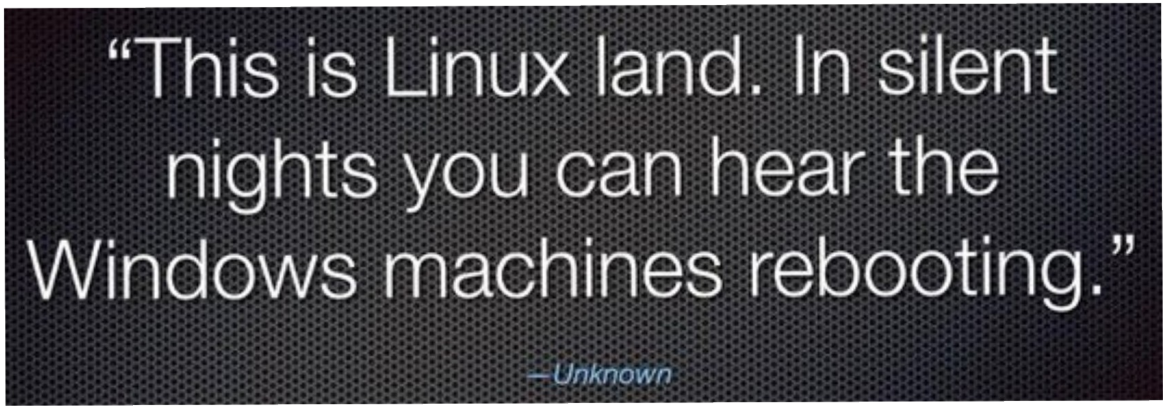
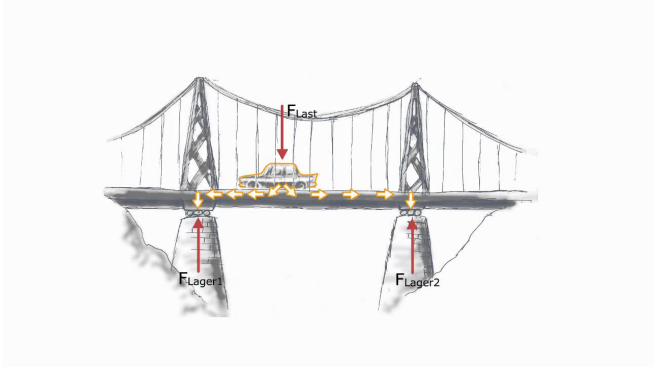
Tor - Netzwerk im Unternehmen

Jean-Claude Kiener
Dipl. Ing. Inf. FH

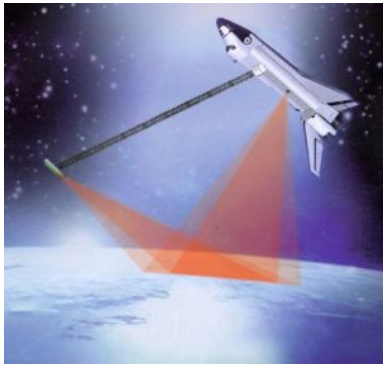
Netzwerk Sicherheitsingenieur
IT Security Specialist / Expert

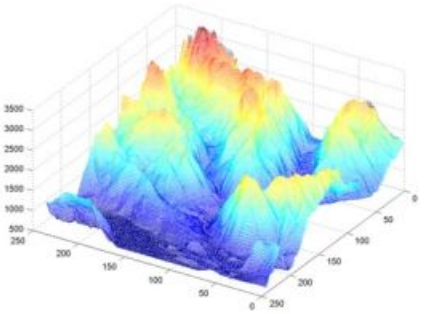


http://www.summo.ch



Jean-Claude Kiener





- IT Forensic
- Incident Response
- Intrusion Detection
- Threat Intelligence
- OSINT (Open Source Intelligence)
- Reverse Engineering
- System- und Netzwerkverantwortlicher

THE **O**nion **R**outing
(Paul Syverson)

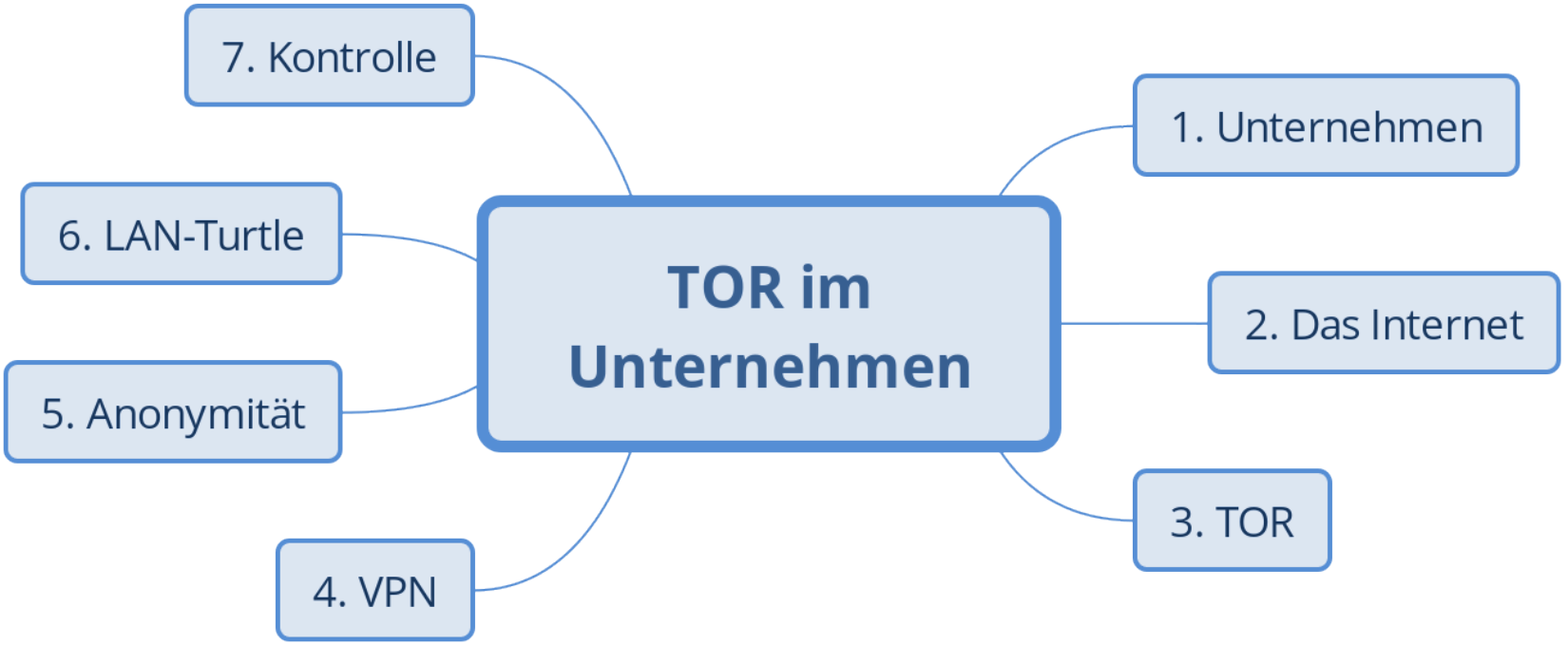
Ein Lösungsansatz kommt aus der militärischen Forschung. Es kam aus der Idee:

« **Electronic Warfare** »
« Elektronische Kampfführung »

Im Mai **1996** wurde das Prinzip des Onion Routings erstmals präsentiert.

Seit Oktober **2003** ist das TOR-Netzwerk Online und bis heute fortwährend erreichbar gewesen.

Inhalt



Was nehmen Sie aus dem Referat mit ?

- Vorteile für das Unternehmen TOR zu verwenden
- Was heisst es sich anonym im Netz zu bewegen

1. Unternehmen

Hürden für die Verwendung von TOR

- Kritische Infrastruktur
- Unternehmensinterne Sicherheitsvorkehrungen
- Internet Policy

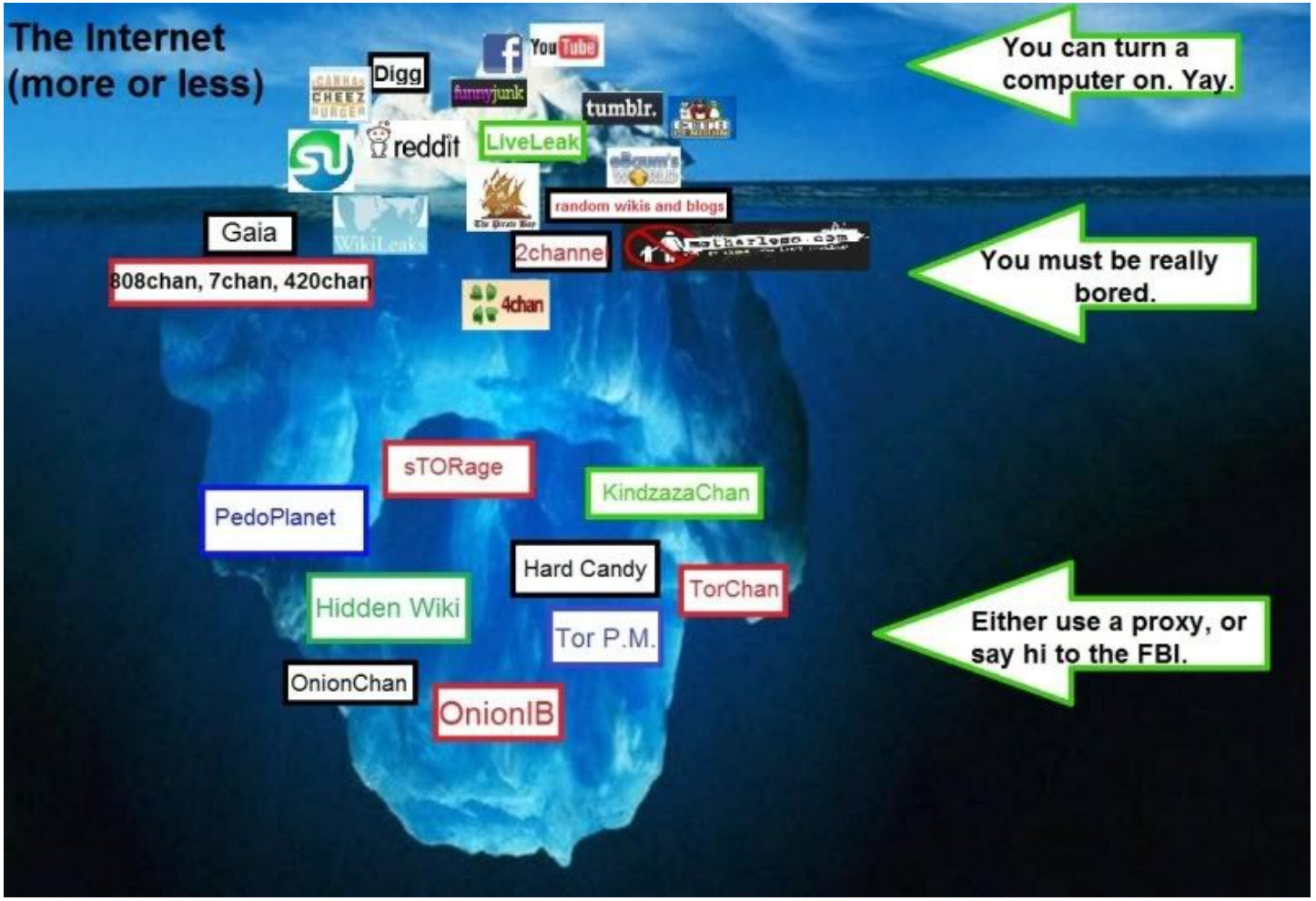
1. Unternehmen

Vorteile von TOR ?

- Anonymität
- Informationsbeschaffung
- Verbreitung von Informationen
- Neugierde
  - bsp. Konkurrenz besuchen
- Vorratsdatenspeicherung umgehen
- Prism (seit 2005) verhindern

2. Das Internet

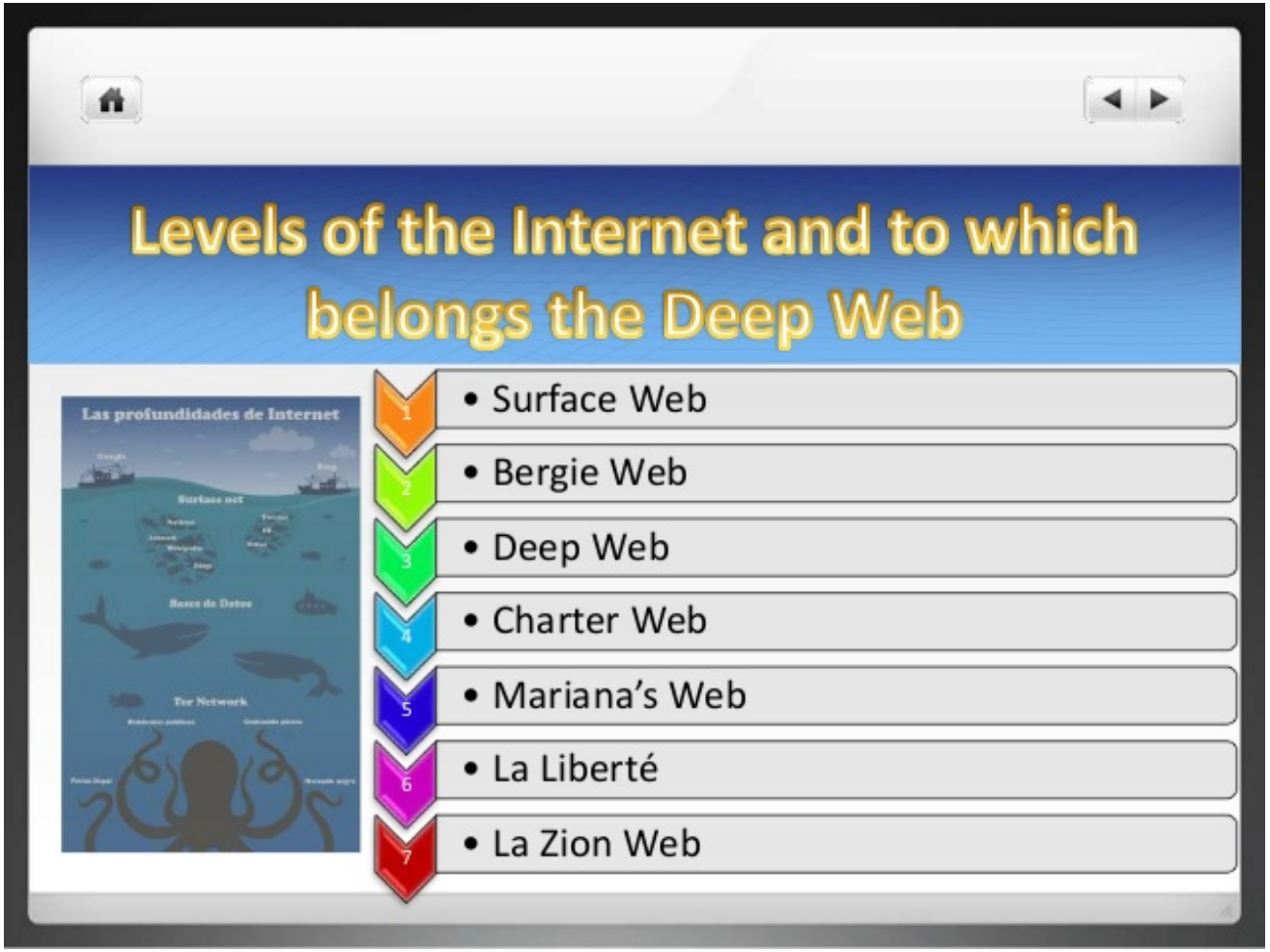
Internet → Deep Web → Darknet ?



Quelle: unbekannt

2. Das Internet

Internet → Deep Web → Darknet ?



Quelle: slideshare.net/albafg55

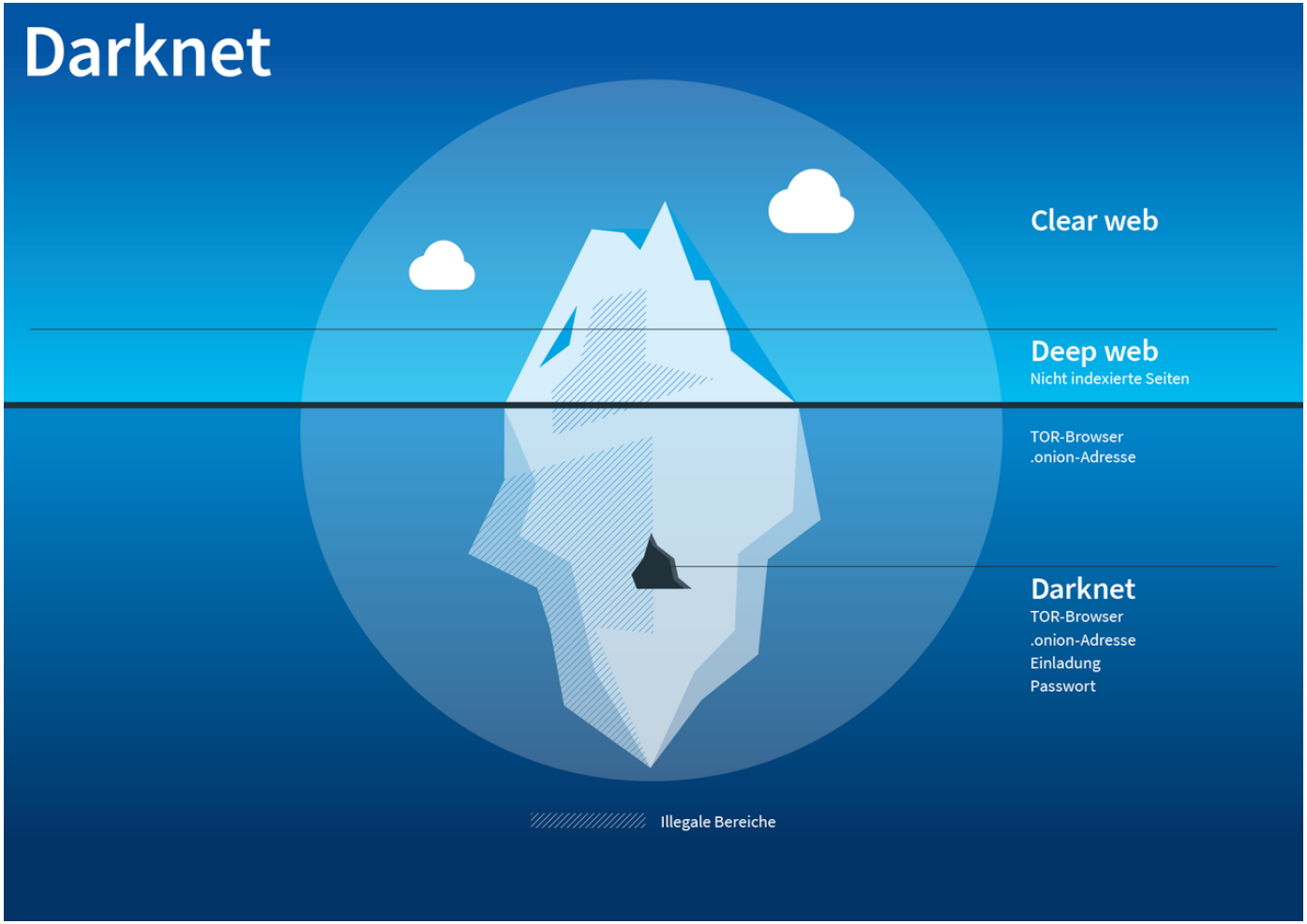
2. Das Internet

Internet → Deep Web → Darknet ?

Clear	Surface Web	Youtube, Instagramm, Twitter, Facebook, etc.
	Bergie Web	4chan, The Pirate Bay, Porn pages, „**jailbait**“
Deep	Deep Web	Hacker, Script Kiddies, Informationen über Viren, Kinderpornographie (leicht)
Darknet	Charter Web	Verbotene Bücher, Kontakt zu Auftragsmörder, Verkauf von Drogen
	Mariana‘s Web	The Hidden Wiki *Eine sehr gefährlich Ebene, der tiefste Teil des Deep Web und wo „nobody wants to enter“*
	La Liberté	Eine französische Seite, eine der tiefsten im tiefen Netz *Nur mit Einladung*
	La Zion Web	Zion schlägt La Liberté in der Tiefe, da La Liberté nur Informationen und Videos enthält, die von Zion veröffentlicht wurden.

2. Das Internet

Internet → Deep Web → Darknet ?

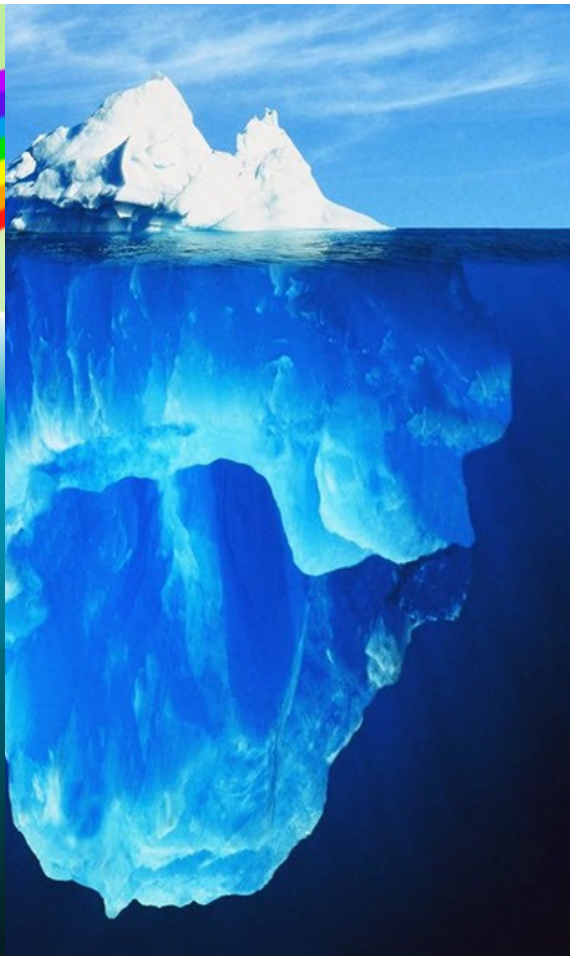


Quelle: gdata.at

2. Das Internet – Wie ich es sehe

Internet → Deep Web → Darknet ?

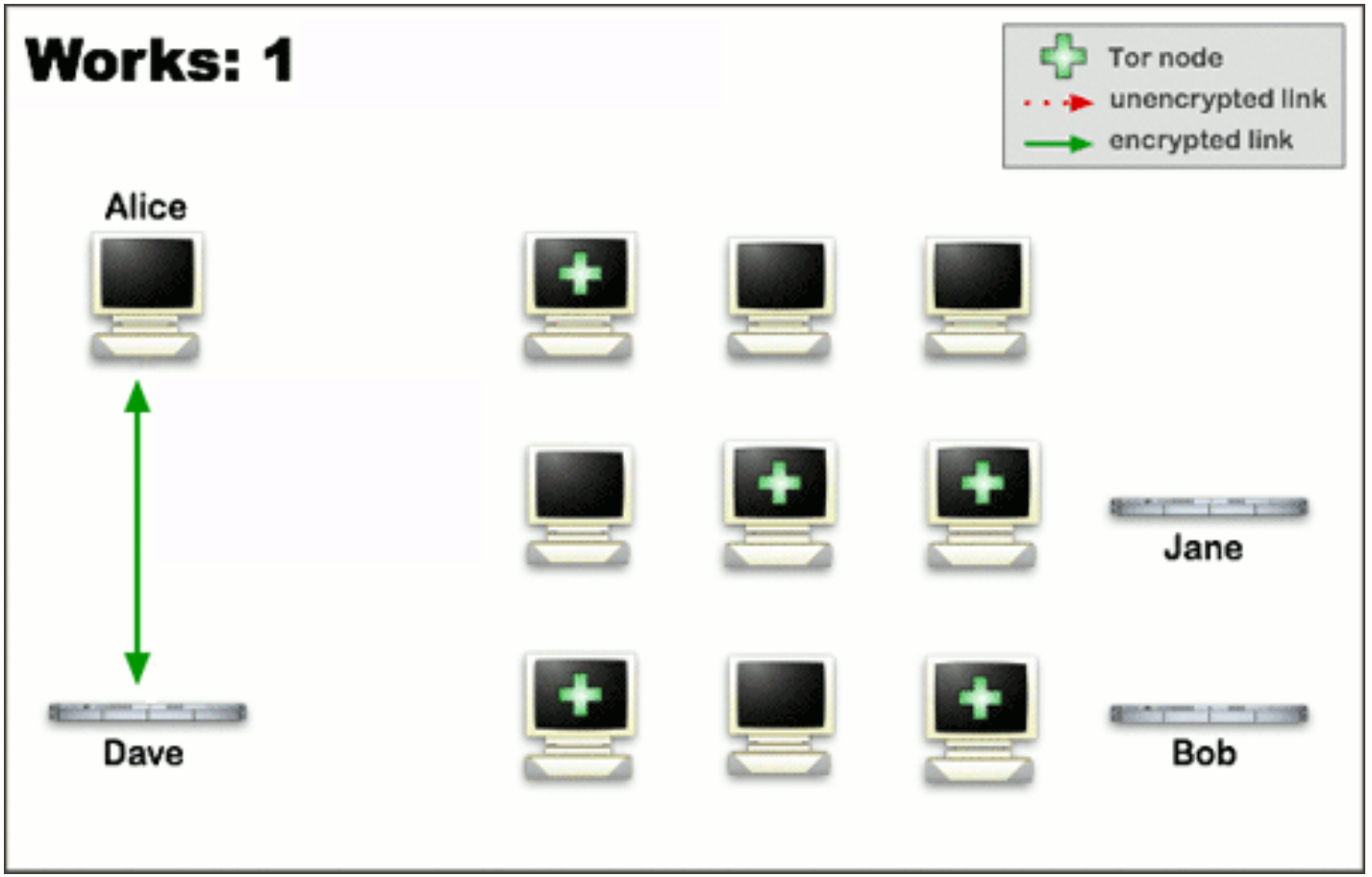
Quelle: bluecoders.io



Quelle: unbekannt

3. TOR – Was man kennt

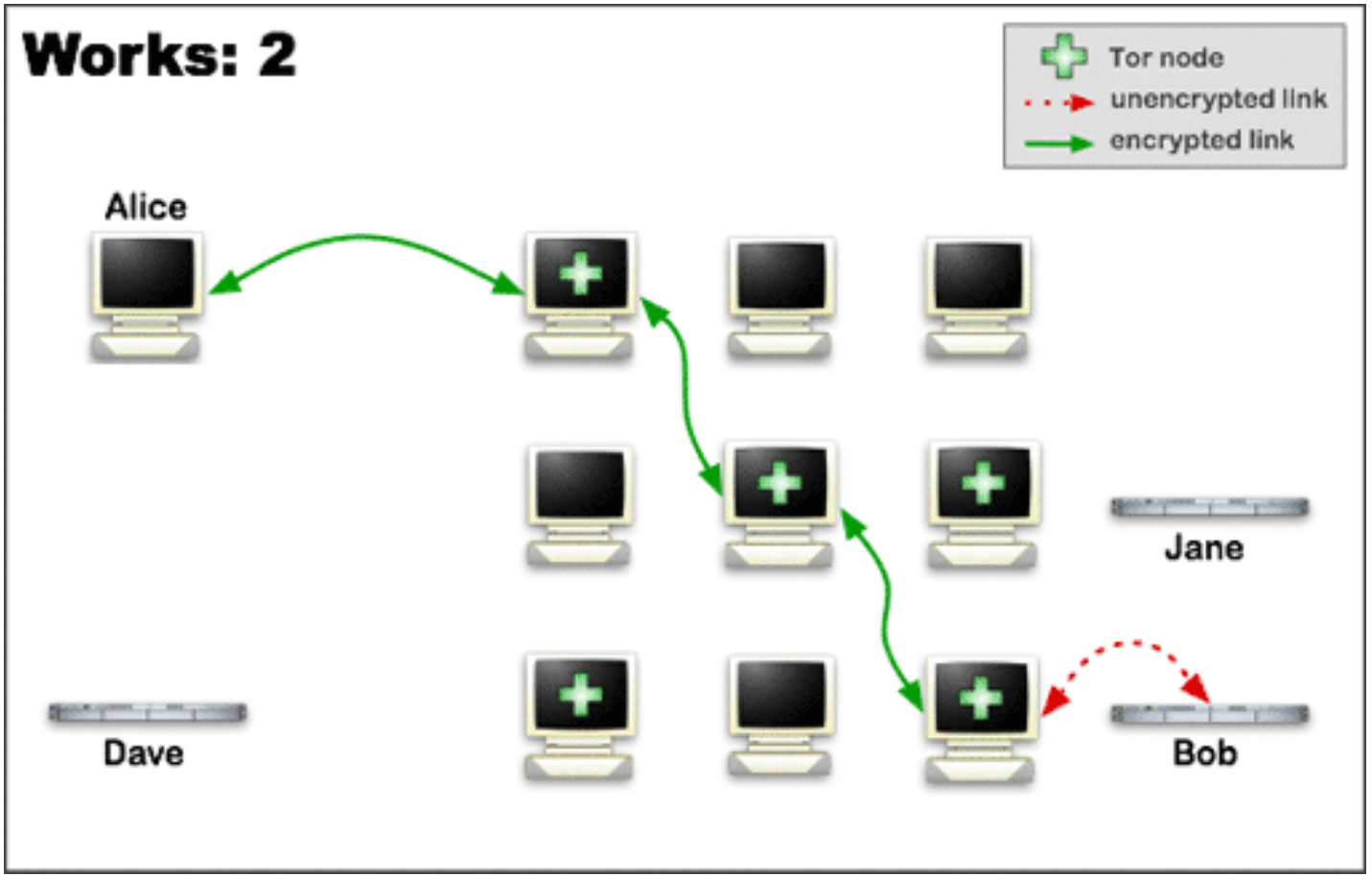
Abholen der Liste



Quelle: eff.org

3. TOR – Was man kennt

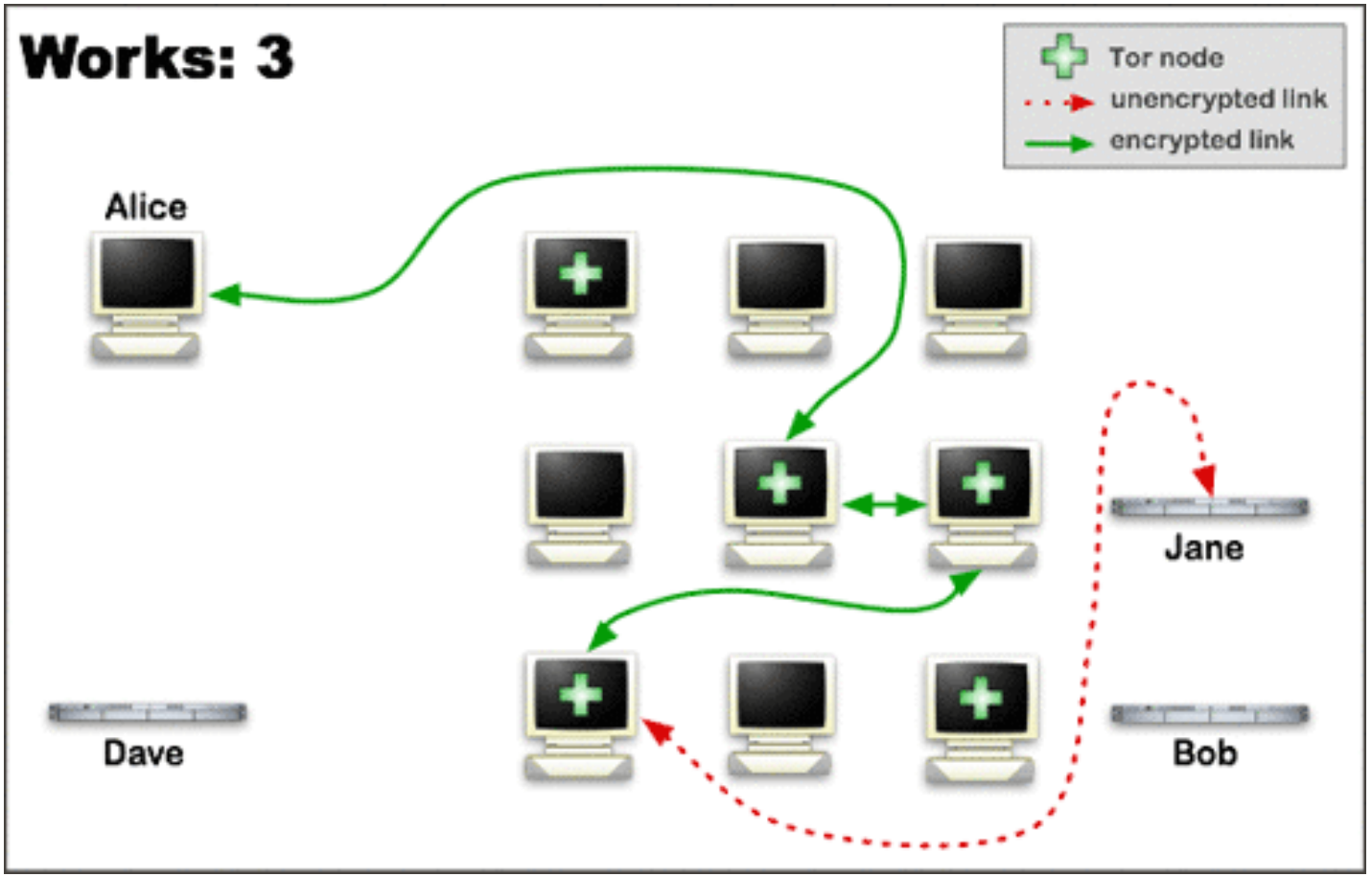
Weg wählen und zugreifen



Quelle: eff.org

3. TOR – Was man kennt

Neuer Weg wählen und zugreifen



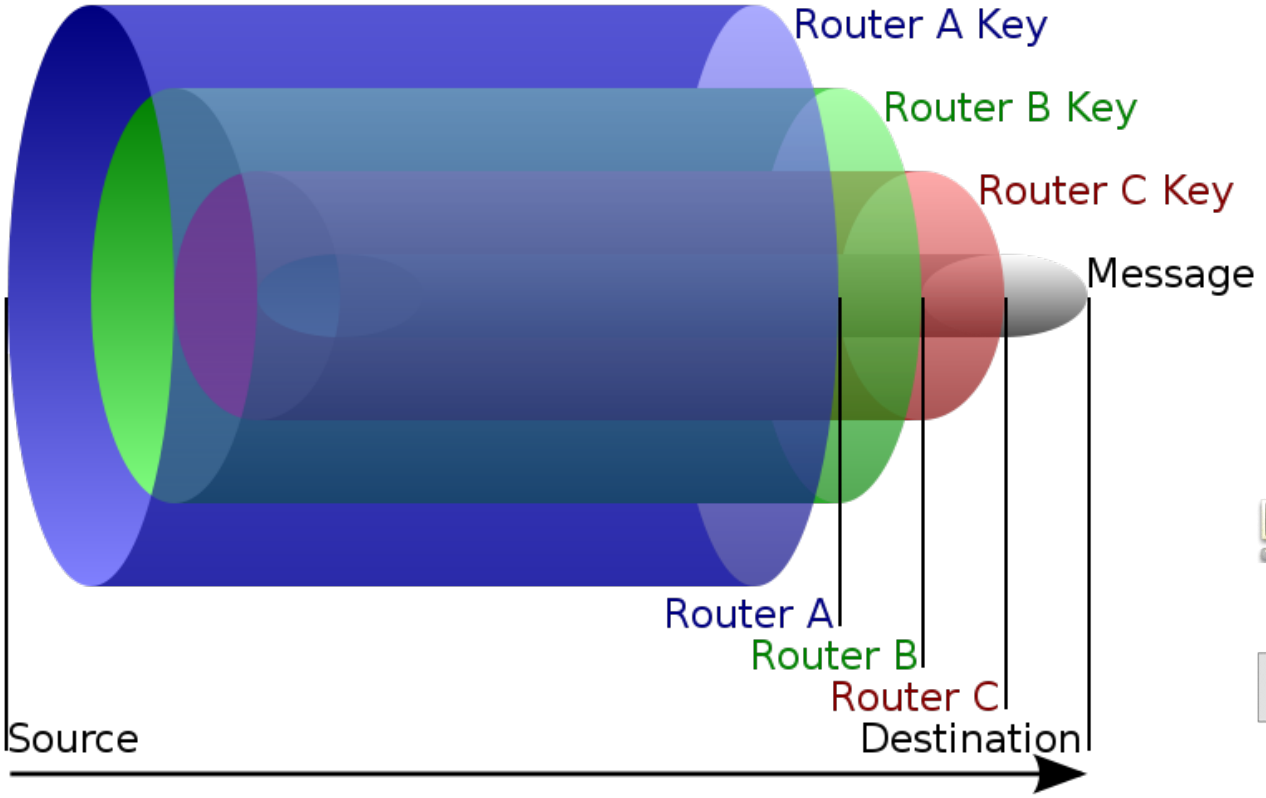
Quelle: eff.org

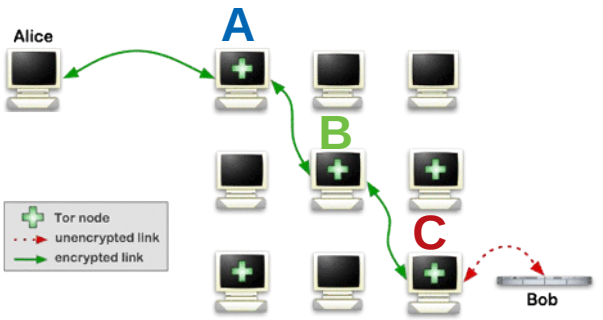
3. TOR – Funktionsweise

Die verschiedenen Server im TOR-Netzwerk

Onionproxy	Ist das Nutzerprogramm
Entryguard	Eintrittspunkt ins Netzwerk
Onionrouter	Weiterleiten der anonymen Verbindungen
Verzeichnisserver	Informationen über die Onionrouter
Kontaktserver	Server um Bob zu verstecken, Alice wird bei der Anfrage an Bob weitergeleitet.
Rendevouspunkt	Schnittstelle zwischen Alice und Bobs versteckten Service
Brückenserver	Bietet Nutzern, deren Internetverbindung zensiert oder stark eingeschränkt ist, einen Zugang zum Netzwerk. **Diese Adressen sind besonders schützenswert !**

3. TOR – Verschlüsselung



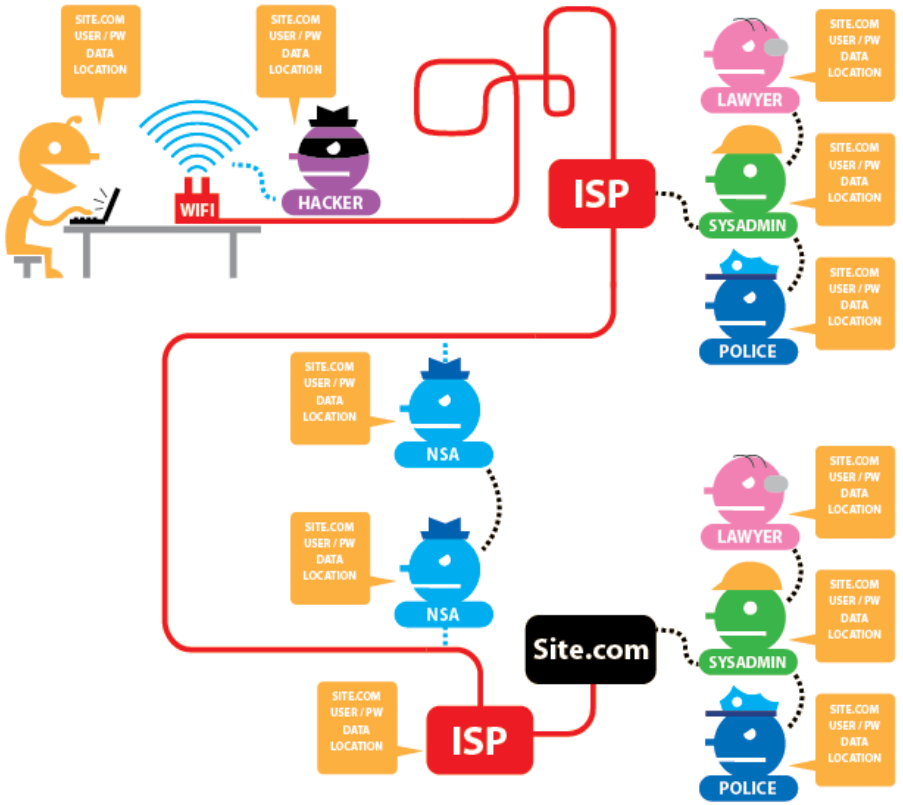


Quelle: wikipedia.org

Quelle: eff.org

3. TOR – Was sehen die anderen?

Tor
HTTPS



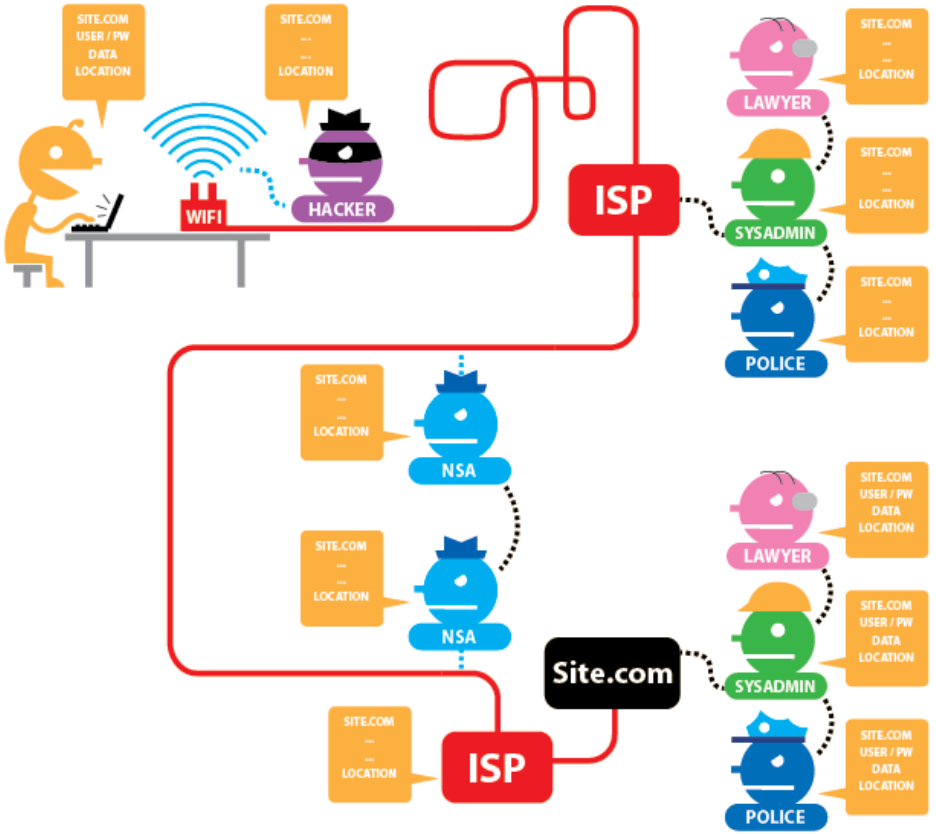
Akteure:
- Benutzer
- Hacker
- Gesetz
- SysAdmin
- Polizei
- NSA

Internetverbindung
Abhören
Daten teilen

Aufgerufene Seite
Benutzername / Passwort
Übertragene Daten
Ihre IP-Adresse

3. TOR – Was sehen die anderen?

Tor
HTTPS

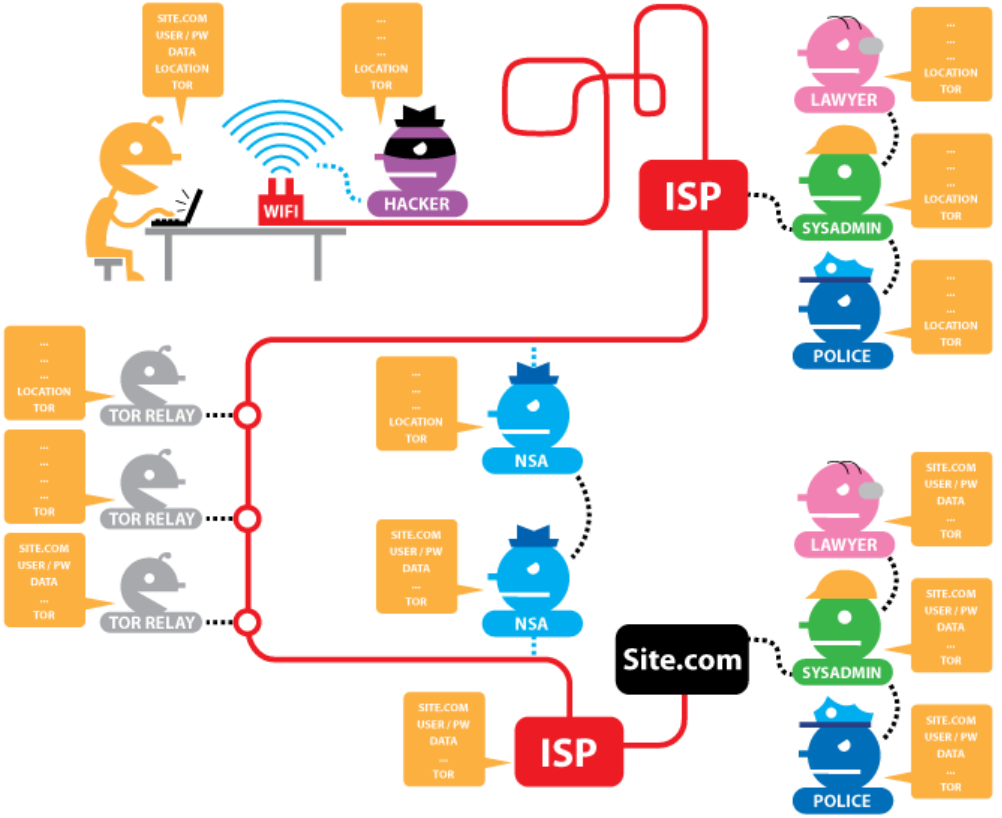


Internetverbindung
Abhören
Daten teilen

Aufgerufene Seite
Benutzername / Passwort
Übertragene Daten
Ihre IP-Adresse

3. TOR – Was sehen die anderen?

Tor
HTTPS



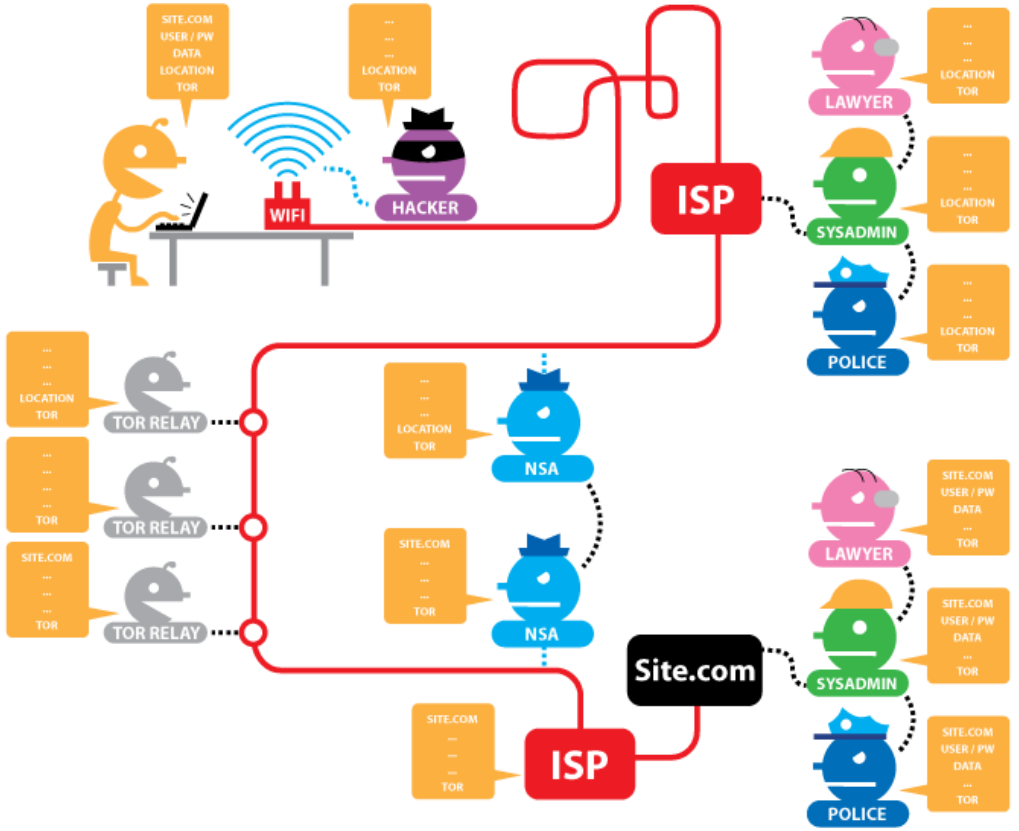
Akteure:
- Benutzer
- Hacker
- Gesetz
- SysAdmin
- Polizei
- NSA
- TOR Relay

Internetverbindung
Abhören
Daten teilen

Aufgerufene Seite
Benutzername / Passwort
Übertragene Daten
Ihre IP-Adresse
TOR

3. TOR – Was sehen die anderen?

Tor
HTTPS



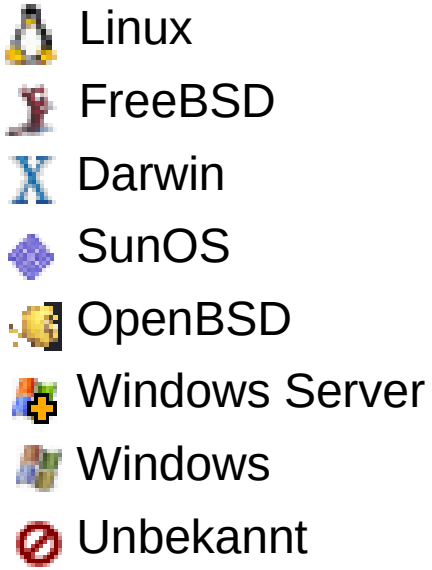
Internetverbindung
Abhören
Daten teilen

Aufgerufene Seite
Benutzername / Passwort
Übertragene Daten
Ihre IP-Adresse
TOR

3. TOR – TOR-Exit-Nodes

Liste der aktuellen Server

https://torstatus.blutmagie.de/



3. TOR – TOR-Exit-Nodes

Weitere Quelle:

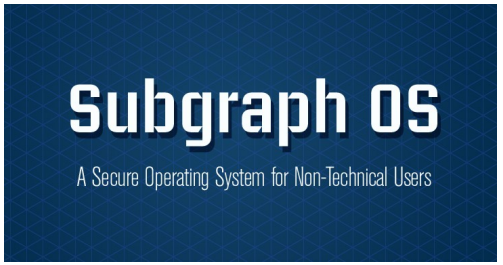
https://metrics.torproject.org/rs.html

TOR-Flow auf einer Weltkarte

(Vorsicht: veraltete Daten)

https://torflow.uncharted.software/

3. TOR – Betriebssysteme



4. VPN – Wahl des VPN-Anbieters

- Keine kostenlosen VPN-Anbieter verwenden !
- Ein VPN-Anbieter muss Folgendes können:
  - Schützen ihrer IP-Adresse
  - Keine LOG-Files aufzeichnen
  - Automatischer Kill Switch
  - Schutz für DNS-Leak
  - Onion Over VPN

4. VPN – Anbieter

Mögliche VPN-Anbieter

- Hide my Ass
- NordVPN
- ExpressVPN
- PrivateVPN
- IPVanish VPN
- Trust.Zone

Ich persönlich verwende:

NordVPN

- ✔ Verschlüsselung 256-AES
- ✔ Keine Logs
- ✔ Bis zu 6 Geräte gleichzeitig
- ✔ Kill Switch
- ✔ Onion Over VPN
- ✔ Akzeptiert Bitcoin

5. Anonymität – Surfen

Tipps

- Sicheres Betriebsystem verwenden
  (Windows gehört nicht wirklich dazu!)
- Nur Software von vertrauenswürdiger Quellen installieren
- Keine verdächtigen Mail-Anhänge öffnen
- Vorsicht beim Besuch von verdächtigen Websites – JavaScript NICHT aktivieren!
- Kommunikation verschlüsseln

5. Anonymität – Erstellen

Was ist hilfreich für eine falsche Identität ?

- Name, Vorname, Ort
- Mail-Adresse

Aufrechterhalten der falschen Identität:

- Nur Angaben verwenden, die **keine Rückschlüsse auf die eigene Person oder das Umfeld zulassen!**

5. Anonymität - Surfen

Worauf muss ich achten ?

- Fenstergrösse (NICHT Vollbild benutzen)
- IP-Adresse
- DNS-Leak
- Nicknames (nicht aus der Privatsphäre)
- Keine Logins mit echten Namen

5. Anonymität – Erstellen

Wie kann man eine korrekte, falsche Identität erstellen?

https://www.fakenamegenerator.com

http://www.datafakegenerator.com/generador.php

5. Anonymität – Vorsicht

Worauf muss bei der Anwendung der Anonymtät dringend geachtet werden?

- IP-Adresse
- DNS-Leak
- Rechtschreibung
- Satzstellung
- Name, Herkunft

5. Anonymität - Einkaufen

- **Bestellen**
  - Anonym, mit falscher Identität
- **Bezahlen**
  - Falsche Kreditkarte
  - Bitcoin
    - Konto eröffnen
    - Konto aufladen
- **Abholung**
  - Briefkasten in der Stadt
  - PickUP-Point (Post)

5. Anonymität – Hochladen

- **Photos**
  - Exif Data Bildinformationen
    (Exchangeable Image File Format)
    - *Datum und Uhrzeit*
    - *Geographische Daten (Geotagging)*
    - *Belichtungsindex (ISO-Wert), Brennweite, Belichtungszeit, Blendeanzahl, etc.*
- **Word / Excel**
  - Beinhalten Metadaten
- **PDF-Files**
  - Können Metadaten enthalten

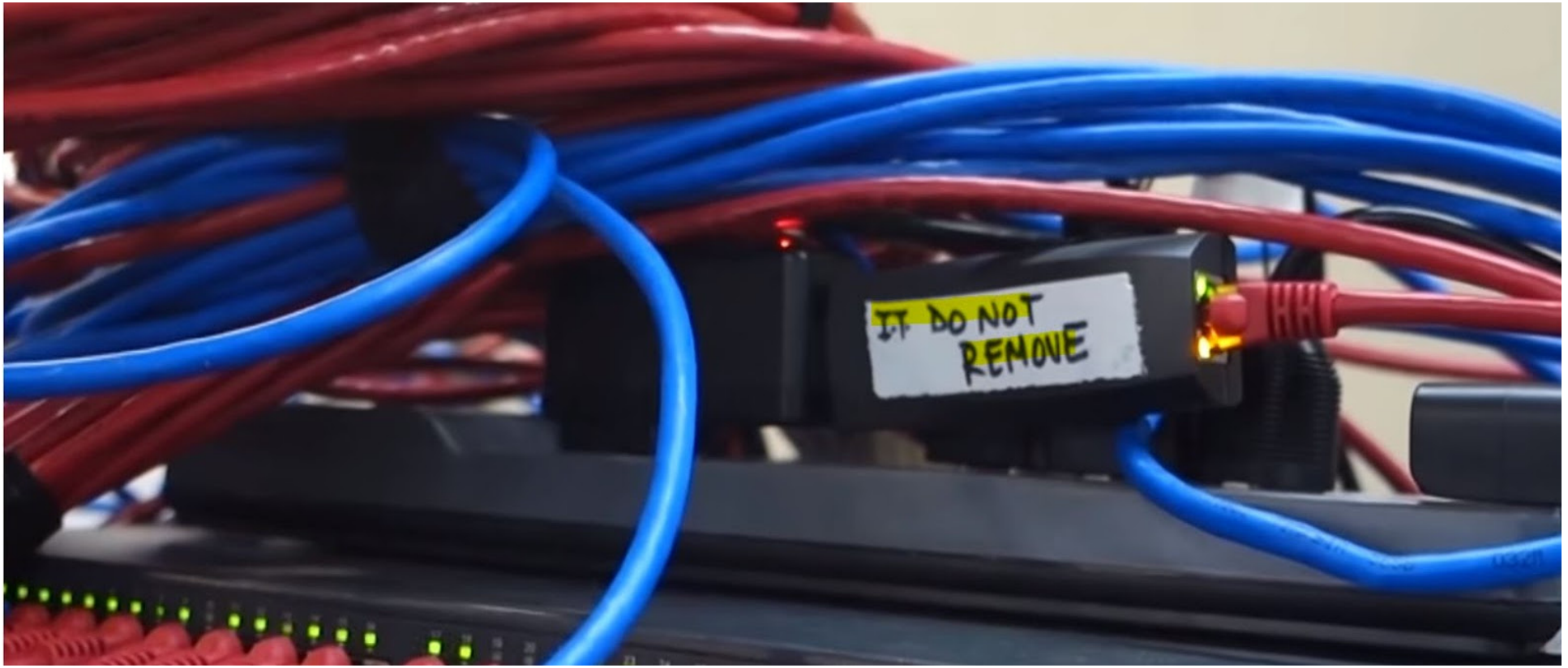
LAN-Turtle

So sieht ein LAN-Turtle auf dem Tisch aus ...

(ältere Version) (neuere Version)

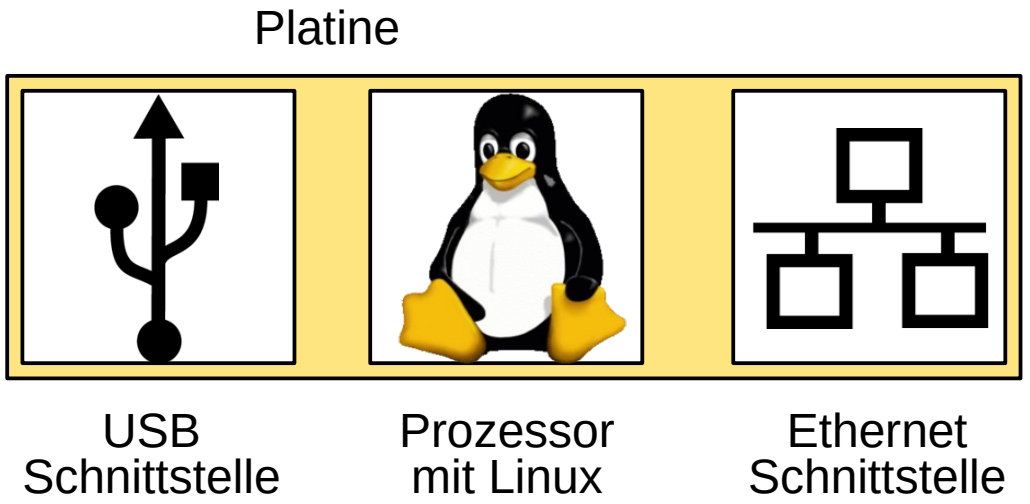
LAN-Turtle

… und so sieht ein LAN-Turtle im Einsatz aus!



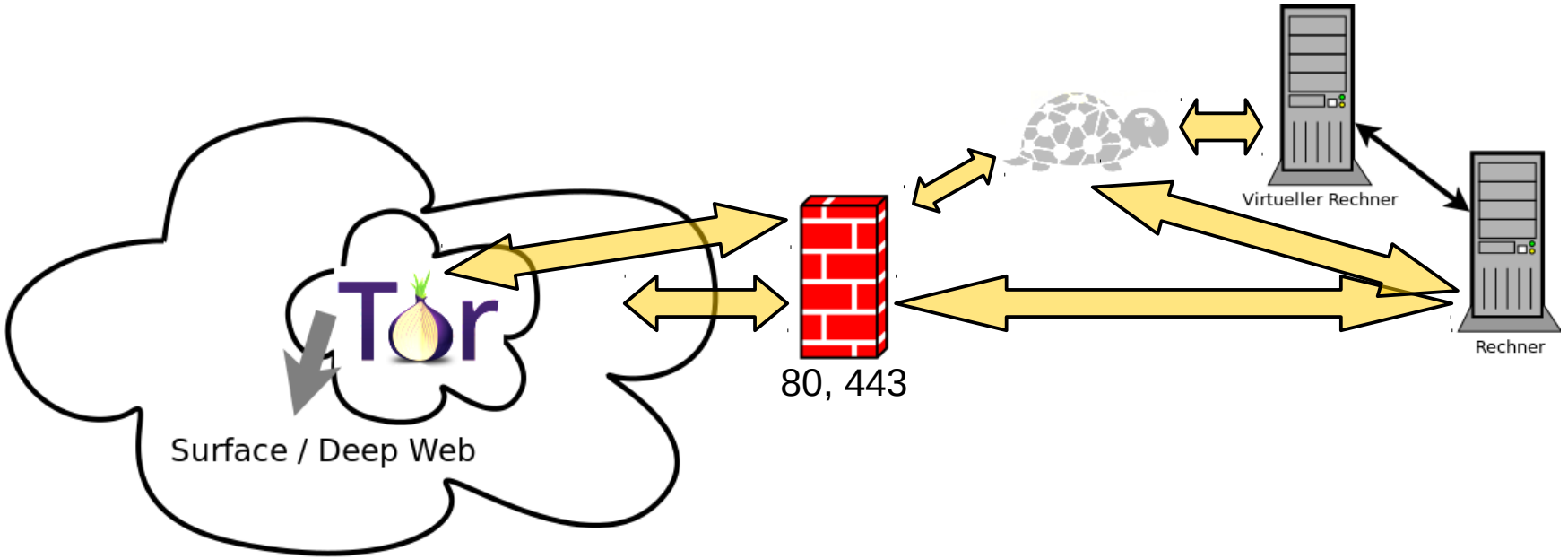
6. LAN-Turtle

Aufbau eines LAN-Turtel‘s

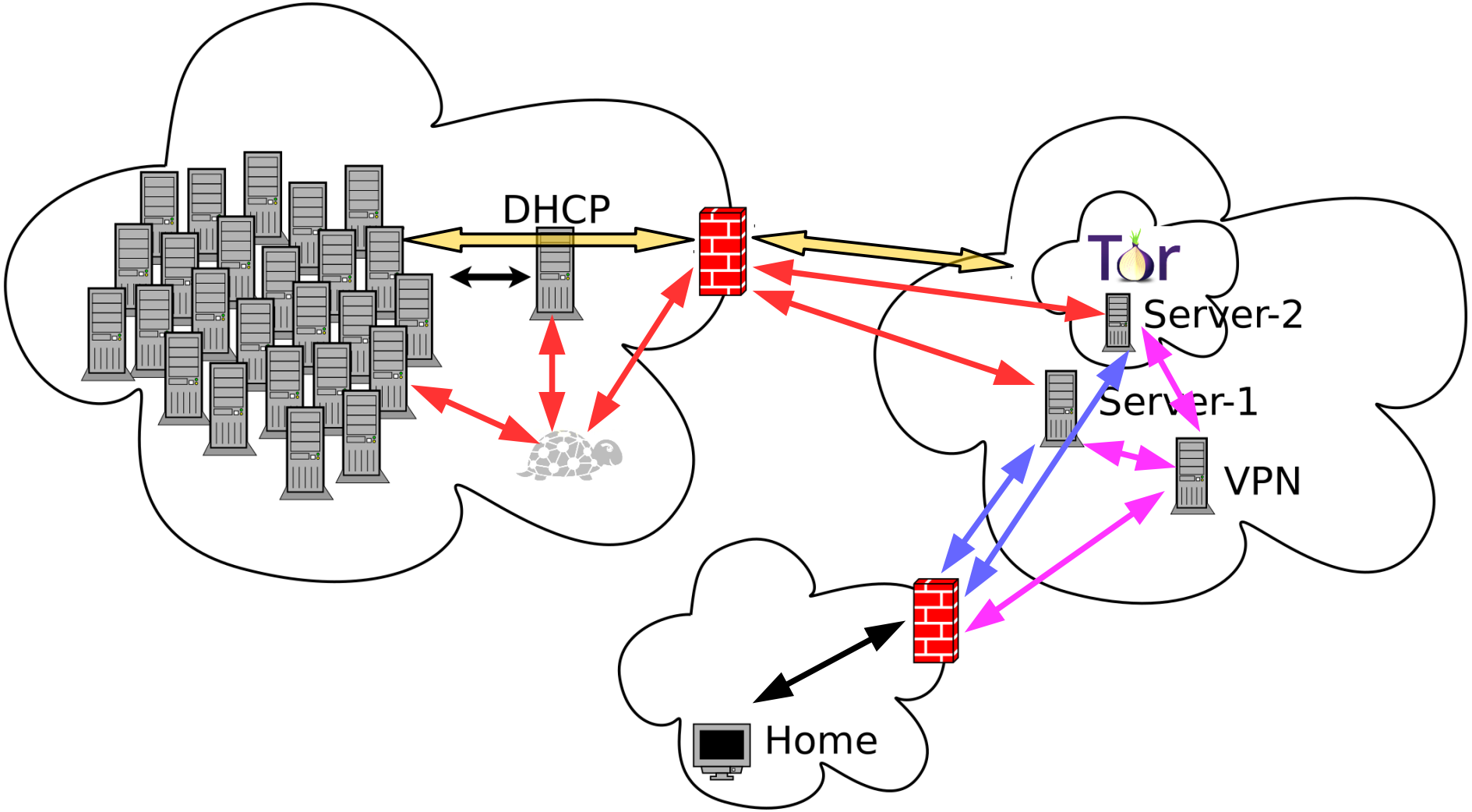


6. LAN-Turtle - Einstieg

Verwendung aus dem eigenen Netzwerk



6. LAN-Turtle – Zugriff

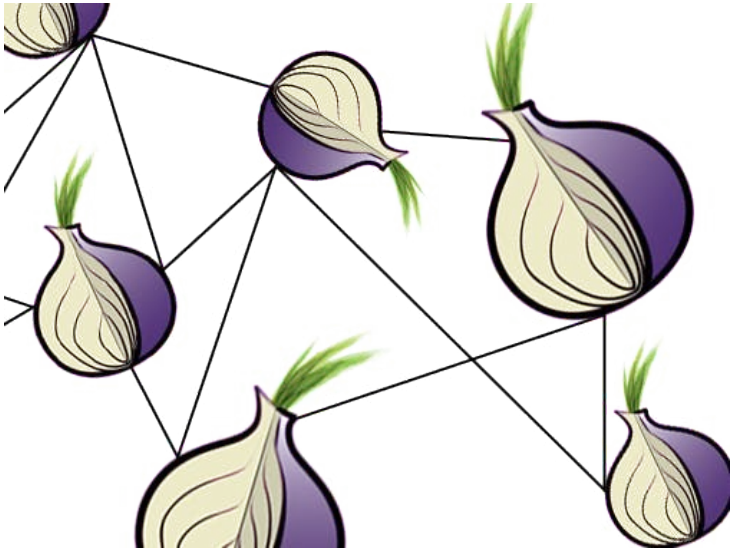


7. Kontrolle

- **Mitarbeiter verwendet TOR**
  - Nutzung der TOR-Netzwerks kann technisch nicht wirklich verhindert werden (Port 80, 443)
  - IP-Adressen statisch vergeben (Nachvollziehbarkeit)
  - MAC-Adressen (Layer 2) analysieren

- **TOR-Adresse greift auf das Unternehmen**
  - Blacklist der TOR-Exit-Nodes

Fragen zum Thema ?



c u another time

s u m m o . c h