ANONYMITÄT IM INTERNET MIT TOR

„Wir verlieren uns in der Menge
keiner kennt unser Gesicht
Ihr werdet niemals wirklich wissen
wer wir sind.“

Die Toten Hosen

PIRATEN PARTEI

ELZPIRATEN EMMENDINGEN

WARUM ANONYMITÄT?

- **„Jeder hat etwas zu verbergen!“**
  - **Bürger**, Journalisten/Informanten:
    - Gesellschaftliche, politische, sexuelle Ausrichtung
    - Aufdecken von Korruption, Steuerhinterziehung, Menschenrechtsverstöße, Umweltzerstörung
  - **Patienten**, Ärzte und Therapeuten:
    - Psychotherapie, Sexueller Missbrauch
    - Schwere Krankheiten wie Krebs, HIV
  - **Mandanten,** Anwälte: z.B. bei Scheidung

→ JEDER SUCHT ZUNÄCHST BEI GOOGLE/IM WEB!?

WARUM ANONYMITÄT?

- **Vorratsdatenspeicherung:**
  - Soll **6 Monate alle Verkehrsdaten** speichern
  - **Verkehrsdaten sind oft aufschlussreicher** als der eigentliche Inhalte!
- **Geheimdienste:**
  - Sammeln seit Jahren **Daten von jedem Einzelnen** in bisher nie gekanntem Ausmaß!
  - Identifizieren einzelne Menschen aus der Masse, um sie zu **verfolgen, zu diskreditieren, zu töten!**

→ NIEMAND KANN SICHER SEIN, WAS IN ZUKUNFT DAMIT GESCHIEHT!

NIEMAND IST ANONYM!

- **Niemand ist im Internet anonym!**
- **Bei jeder Nutzung:** IP-Adresse, Browser, OS ...
- **Website Visitor Tracking:**
  - Analyse des Nutzungsverhaltens auf Websites, Welche Seiten, wann, wie oft, was geklickt wird etc.
- **Dienste:** Google Analytics, Adobe Marketing Cloud, eTracker, DoubleClick, Apple iAd ...
  - Tracking ist sehr einfach umzusetzen, daher weit verbreitet, nutzt fast jede Website

NIEMAND IST ANONYM!

- **Browser Fingerprinting:**
  - Identifizierung auch **ohne IP-Adresse, Cookies** etc.
  - **Studie, Henning Tillmann, 2013:**
    - **Vier Merkmale:** installierte Plug-ins, Schriftarten, unterstützte Dateitypen und User-Agent String
    - **93 %** der Nutzer sind eindeutig identifizierbar
    - http://henning-tillmann.de/2013/10/browser-fingerprinting
    - http://bfp.henning-tillmann.de/
  - **EFF Projekt „Panopticlick“:**
    - https://panopticlick.eff.org/
    - https://panopticlick.eff.org/browser-uniqueness.pdf

NIEMAND IST ANONYM!

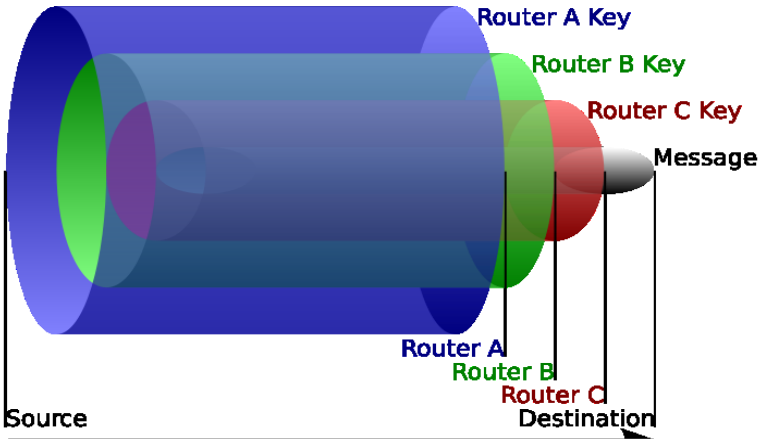
EINDEUTIG IDENTIFIZIERBAR AUS 4 MIO. NUTZERN! :-(

→ Je mehr Browser Plug-ins und Schriftarten etc. desto leichter identifizierbar :-(

WAS IST TOR?

- Netzwerk von virtuellen Tunneln im Internet
- Ursprünglich 2002 von U.S. Navy entwickelt
- Heute: Open-Source Software
  für Windows, Mac, Linux und Android
- Für Web-Browser, Instant Messaging etc.
- Tor = **The Onion Router**

TorProject.org



https://commons.wikimedia.org/wiki/File:Onion_diagram.svg

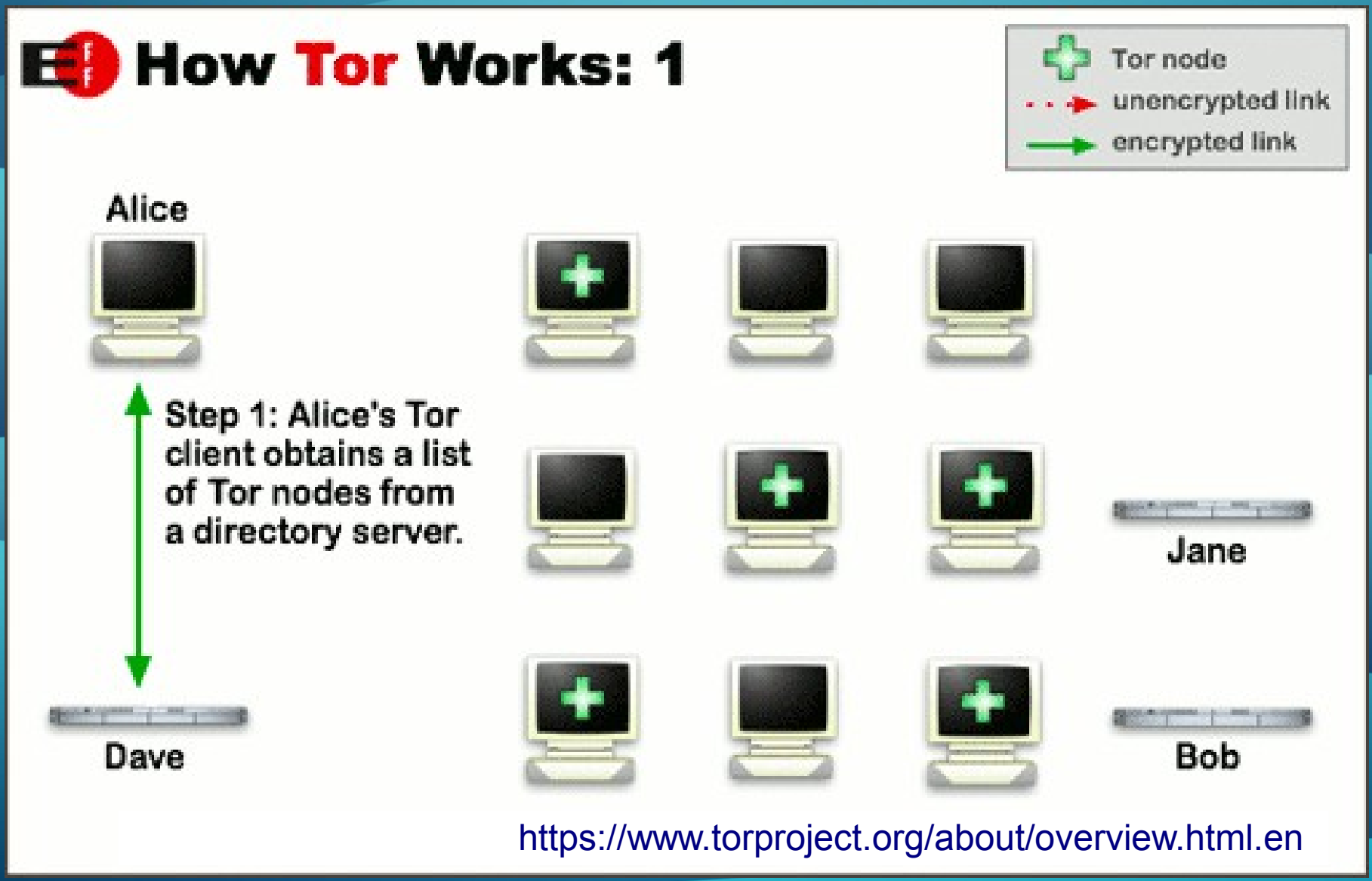
WIE FUNKTIONIERT TOR?

- **Mehrfache Verschlüsselung**
  - Daten sind im Tor-Netzwerk nicht einsehbar

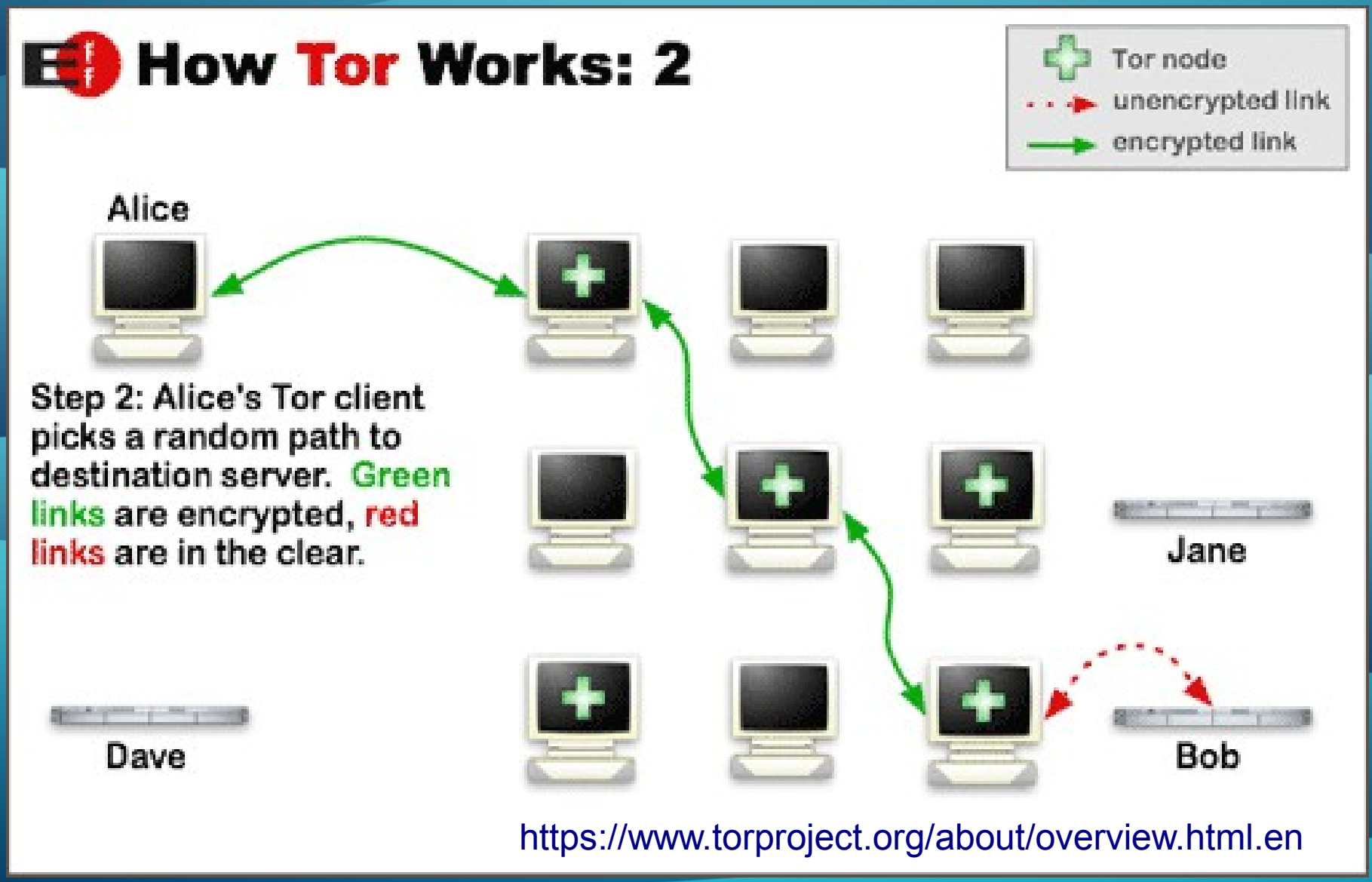
  → Betreiber und Nutzer können im Netzwerk nicht nachvollziehen, *wer mit wem was* kommuniziert.
- **Ständiges Wechseln von Netzwerk-Knoten**
  - Jede Anfrage an einen Server kommt von vermeintlich unterschiedlichen Nutzern
  - Nutzer können selbst eigenen Knoten betreiben

→ NIEMAND KANN MEHR HERAUSFINDEN, WER WELCHE DATEN ANFRAGT.

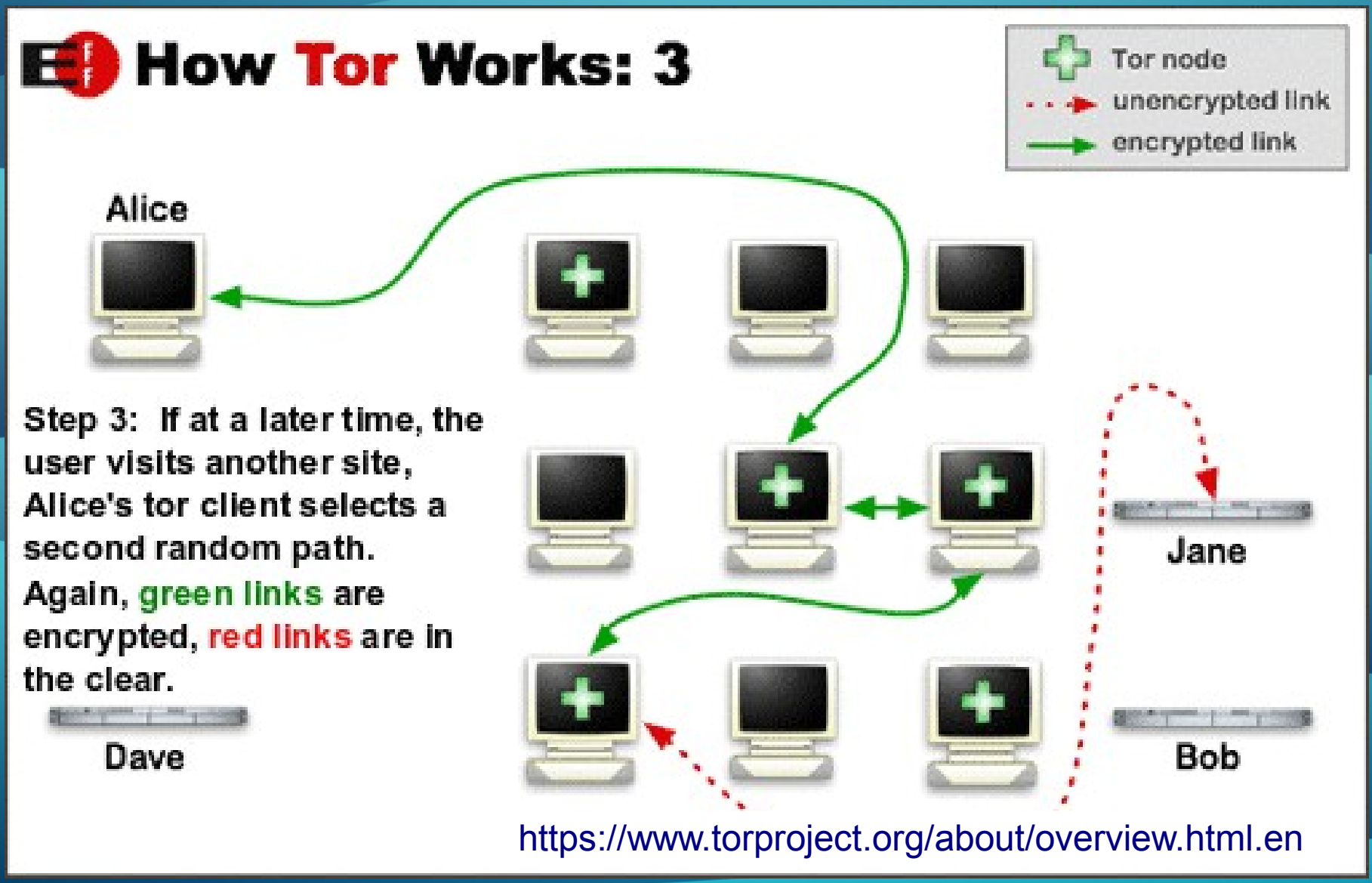
WIE FUNKTIONIERT TOR?



WIE FUNKTIONIERT TOR?



WIE FUNKTIONIERT TOR?



TOR BROWSER BUNDLE

- https://www.torproject.org/download/download-easy.html.en
  - Am besten die **englische Version** verwenden!
- Basiert auf **Firefox** und Add-Ons:
  - TorLauncher + TorButton
  - HTTPS-Everywhere
  - NoScript (JavaScript abgeschaltet)

- **Für Windows, Linux, OS X**

→ KEINE KONFIGURATION NOTWENDIG :-)

TOR BROWSER BUNDLE

BEI 4 MIO. NUTZERN GIBT ES 4000 ANDERE MIT DEN GLEICHEN EIGENSCHAFTEN

→ Mit dem Tor Browser sinkt die Wahrscheinlichkeit eindeutig identifiziert zu werden deutlich :-)

BEITRAGEN: TOR RELAY

- **Windows:** Vidalia Relay Bundle (GUI) installieren
  https://www.torproject.org/download/download.html.en
- **Debian/Ubuntu:** Tor per **apt-get** installieren
  https://www.torproject.org/docs/debian.html.en
  (**Nicht** die Pakete aus dem Ubuntu Universe verwenden!)
- **OS X:** Tor mit **Homebrew** installieren
  https://www.torproject.org/docs/tor-doc-osx.html.en
- **Als Tor Relay konfigurieren:**
  https://www.torproject.org/docs/tor-doc-relay.html.en

→ JE MEHR TOR RELAYS, DESTO BESSER WIRD DIE ANONYMITÄT FÜR ALLE TOR NUTZER!

TOR BRIDGE RELAYS

- Relays, die **nicht im Tor Netzwerk gelistet** sind.
- Internet Provider erkennen und blockieren Netzwerkverkehr von Tor.
- **Obfuscated Bridges:** Tor Netzwerk Verkehr wird verschleiert: schwerer zu erkennen.
- https://www.torproject.org/docs/bridges.html.en
- https://bridges.torproject.org/

→ NUR WENN MIT DEM TOR BROWSER KEINE VERBINDUNG AUFGEBAUT WERDEN KANN, SOLLTEN BRIDGES VERWENDET WERDEN!

TOR HIDDEN SERVICES

- Web Server, die **nur innerhalb des Tor Netzwerkes** bekannt sind. Der Web Server darf **nur als localhost** zugänglich sein!
- Hidden Service wird in **torcc** konfigueriert:

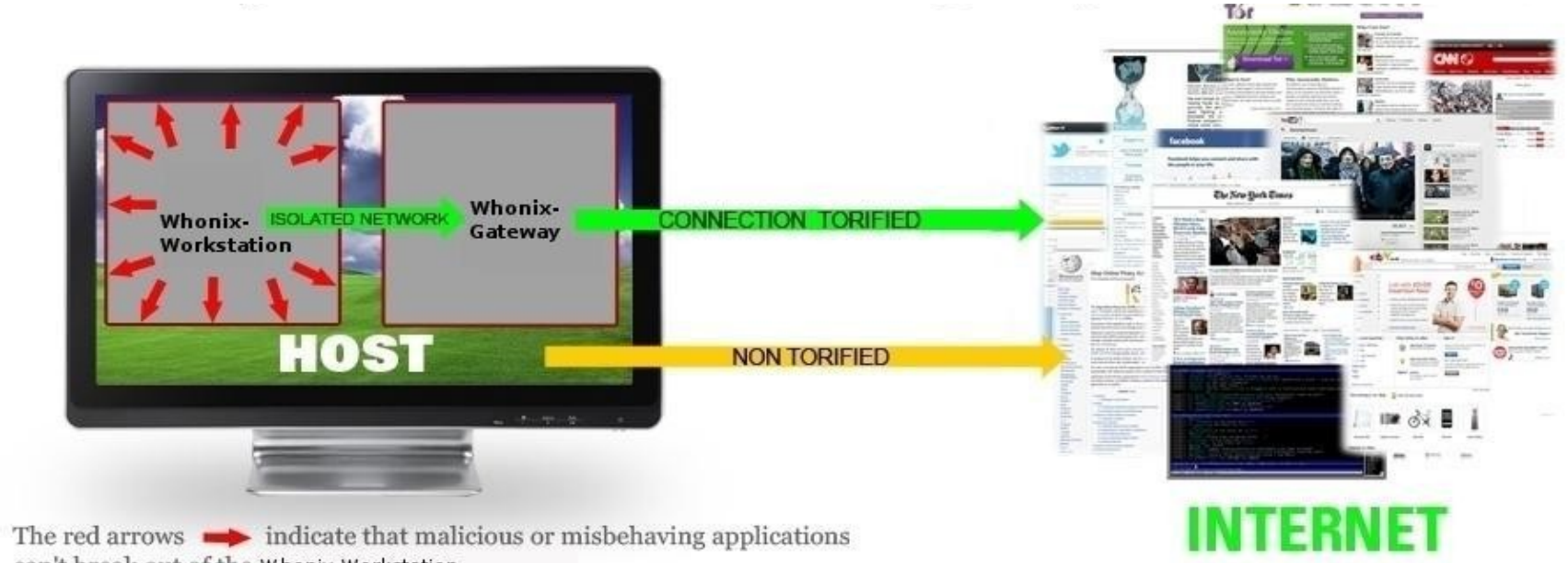
```
HiddenServiceDir /home/username/hidden_service/
HiddenServicePort 80 127.0.0.1:8080
```

- Tor legt dann zwei Dateien an:
  - **private_key**: geheim!
  - **hostname**: z.B. `duskgytldkxiuqc6.onion`, öffentlich!
- Nur den **Hostname** an andere Nutzer weitergeben!

https://www.torproject.org/docs/tor-hidden-service.html.en

WHONIX

- Linux Distribution, mit Fokus auf Anonymität, Privatsphäre und Sicherheit
- Verbindungen ins **Internet nur über Tor**:



- https://www.whonix.org/wiki/Main_Page

WARNUNG!!

- Tor ist **nicht für das alltägliche Surfen** gedacht, sondern für Fälle, in denen Anonymität zwingend notwendig ist!
- Die Nutzung von Tor ist durch die mehrfache Weiterleitung **langsamer als gewohnt**.
- **Nur den Tor-Browser verwenden**, keine zusätzlichen Plug-ins wie Flash installieren!
- **Immer HTTPS nutzen**, Daten verschlüsseln!

WARNUNG!!

- Tor **niemals für Facebook/Twitter**... mit realer Identität nutzen! (Wenn: jew. neuer Account)
- **Keine persönliche Daten** (Alter, Namen, PLZ, E-Mail, Mobilfunk-Nr...) eingeben!
- Tor **nie für Online-Banking**, Paypal, Kreditkarte oder Online-Shopping nutzen! (Bankkonto kann wegen Betrugs gesperrt werden!!)
- **Nie die eigene Website**/Profil anschauen, nach eigenem Namen googlen... auch nicht nach Kollegen, Freunde, Verwandte! **Keine Namen!**

WARNUNG!!

- **Keine Dokumente** (doc, pdf) direkt öffnen, während man anonym online ist!
  - Dokumente könnten Daten außerhalb von Tor aus dem Internet laden und die Anonymität brechen!
  - Dokumente nur offline auf einem anderen Rechner oder in virtueller Maschine ohne Internet nutzen!
- **Kein TORRENT-Filesharing** über Tor nutzen:
  - Die eigene IP-Adresse steht in den GET-Requests
  - Filesharing verlangsamt das Tor-Netzwerk!

WEITERE HINWEISE

- Weitere Links und Hinweise zum Umgang mit Tor:
  - http://artikel.softonic.de/anonym-surfen-so-funktioniert-der-tor-browser
  - https://www.torproject.org/about/overview.html
  - https://www.torproject.org/download/download-easy.html.en#warning
  - https://www.whonix.org/wiki/DoNot

VIELEN DANK!

"We will never be able to de-anonymize all Tor users all the time,"

GCHQ

FRAGEN?