WOLLEN WIR DAS DARKNET?

Dr. Rüdiger Peusquens

Bonn, 08.03.2018

ERLEBEN, WAS VERBINDET.

DARKNET

WAS IST DAS EIGENTLICH?

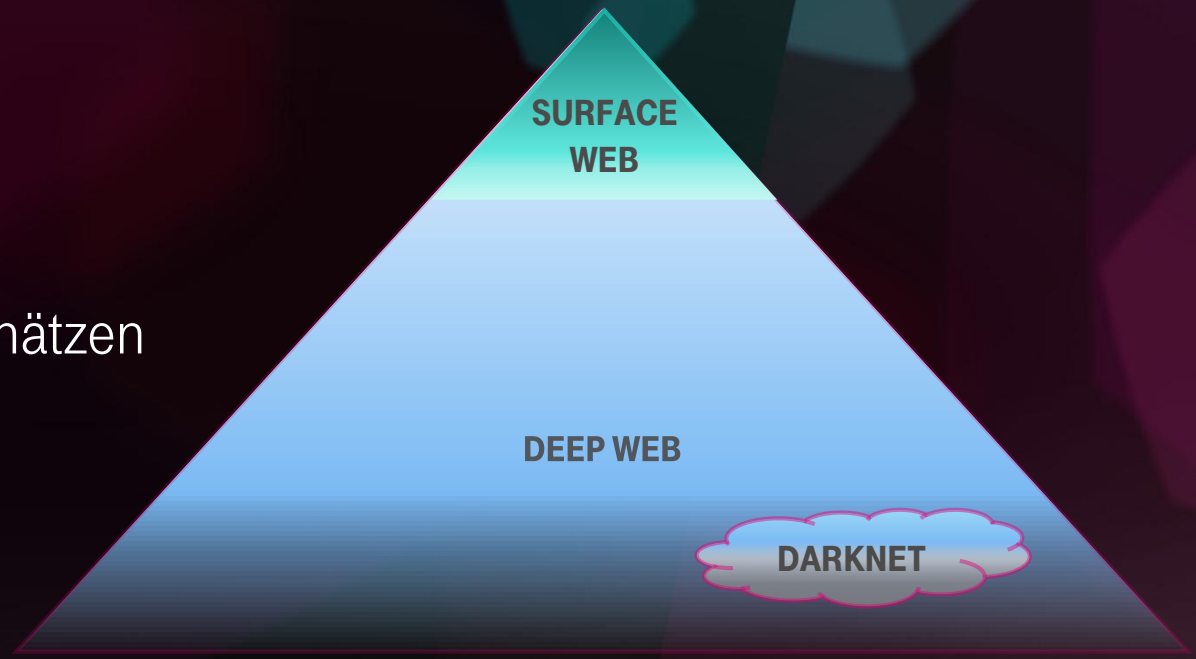
Nischen im World Wide Web

sichtbar

vs.

verborgen

MEHR ALS GOOGLE: SCHICHTEN DES WORLD WIDE WEB



Surface Web: Durch Suchmaschinen indiziert

Deep Web: Größer als Surface Web, schwer zu schätzen

- Dynamische Webseiten
- Blockierte, nicht verlinkte und private Seiten
- Netzwerke mit eingeschränktem Zugang
- Seiten mit nicht-standard DNS, TLDs: Zugang nur mit Kenntnis oder spezielle Ressourcen
- Nicht-HTML Inhalte und andere Protokolle

Darknet: Manuelle Vernetzung

z.B. über gekapselte Software (Tor, I2P, Freenet, GNUnet, RetroShare)

DEEP WEB, EIN PRIVATES BEISPIEL

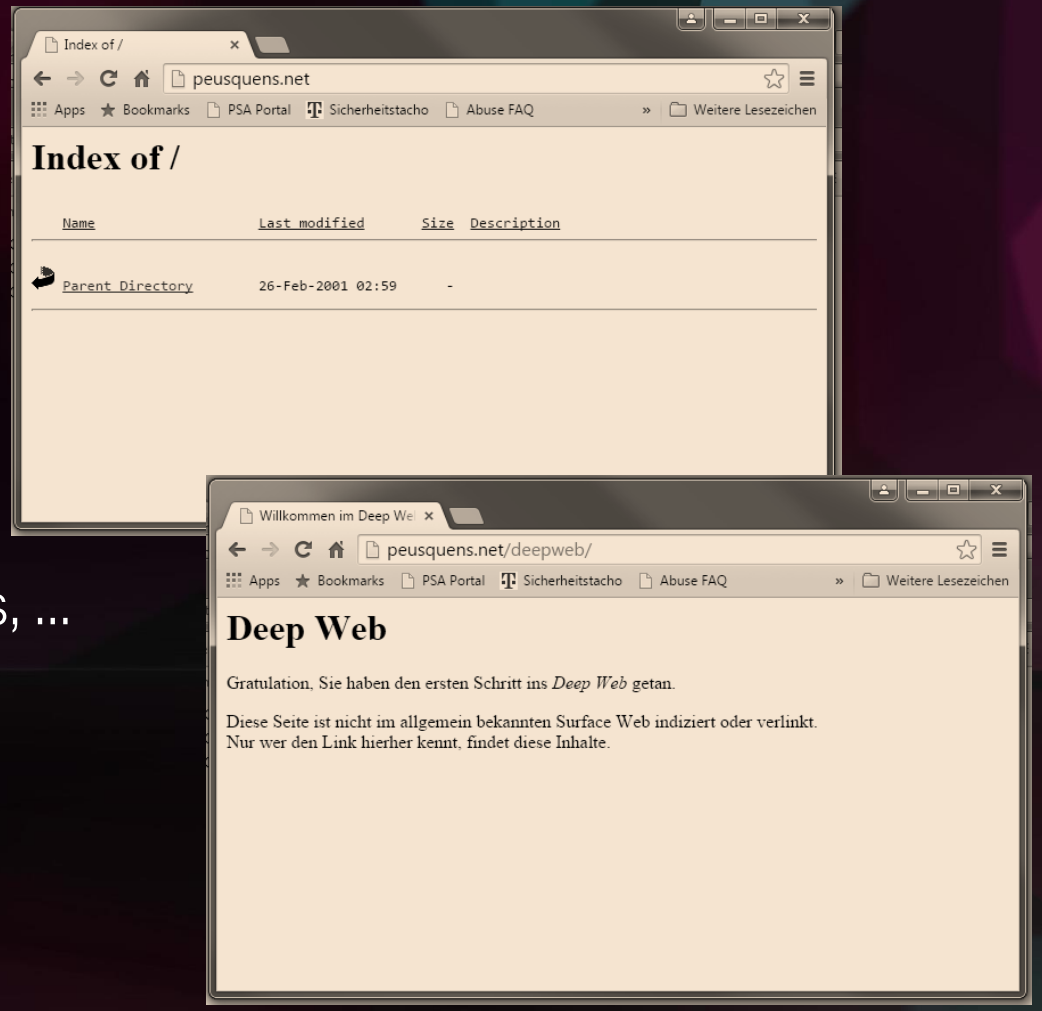
www.peusquens.net ?

www.peusquens.net/deepweb !

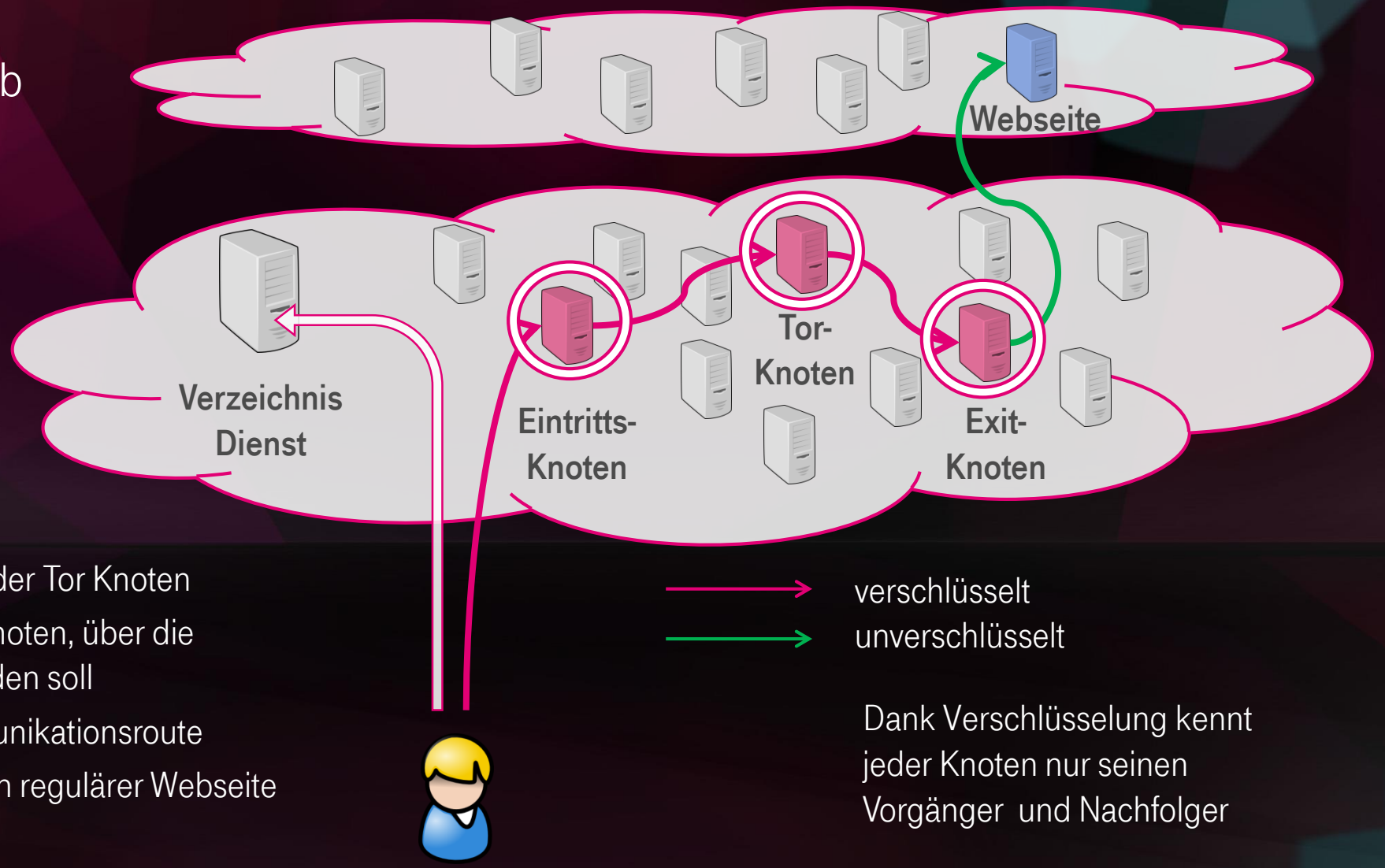
- nicht bei Google, Bing, Yahoo, ... indiziert
- nicht verlinkt von anderen Seiten

Deep Link: wer es kennt, findet Jahrgangsseite, Fotos, ...

→ einfacher Ansatz, Inhalte zu verbergen
geringer Schutz (Obscurity statt Security)



ANONYME VERBINDUNG MIT THE ONION ROUTING (TOR)



1. Abfrage existierender Tor Knoten
2. Auswahl der Tor Knoten, über die kommuniziert werden soll
3. Aufbau der Kommunikationsroute
4. Anonymes Aufrufen regulärer Webseite

verschlüsselt
unverschlüsselt

Dank Verschlüsselung kennt jeder Knoten nur seinen Vorgänger und Nachfolger

THE ONION ROUTING (TOR NETZWERK)

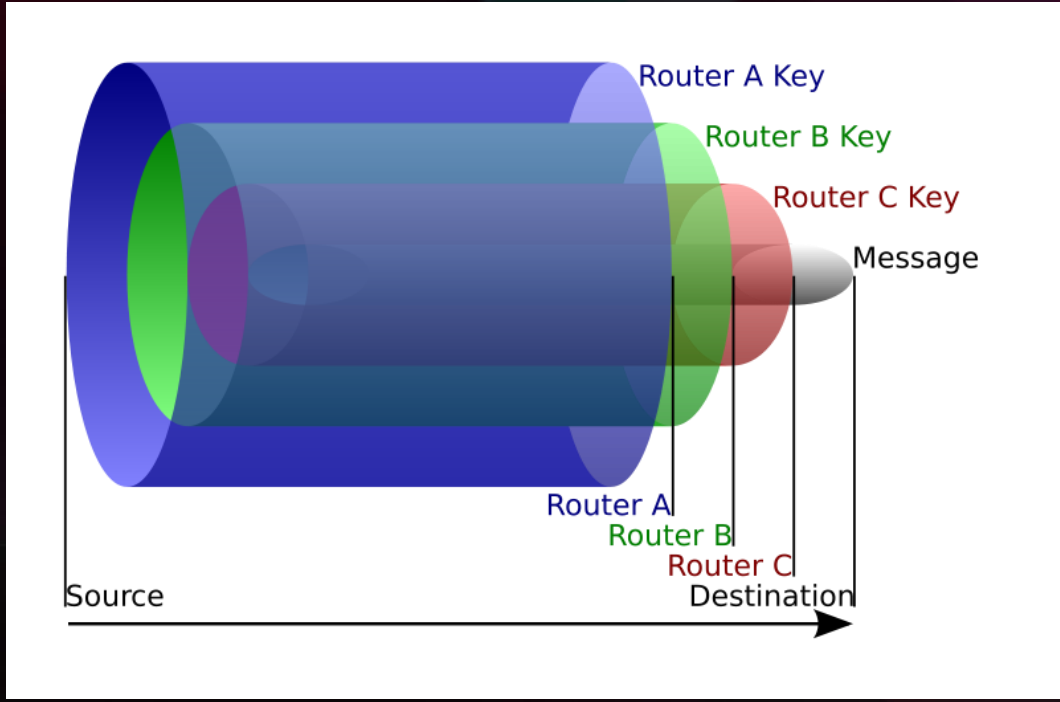
Daten werden in Schichten verschlüsselt.

Schlüssel hängen vom gewählten Weg ab.

Jeder Knoten kann nur die für ihn bestimmte Schicht entschlüsseln und die resultierenden Krypto-Daten an den nächsten Knoten weiterleiten.

Jeder Knoten kennt nur den Vorgänger und Nachfolger

Tor gewährleistet Anonymität aber nicht Vertraulichkeit
Exit-Node sieht Verbindungsziel und Inhalt



Autor: HANtwister, Quelle: http://en.wikipedia.org/wiki/Image:Onion_diagram.svg

EINFACHE NUTZUNG MIT DEM TOR-BROWSER

Software im Internet frei (und legal) verfügbar

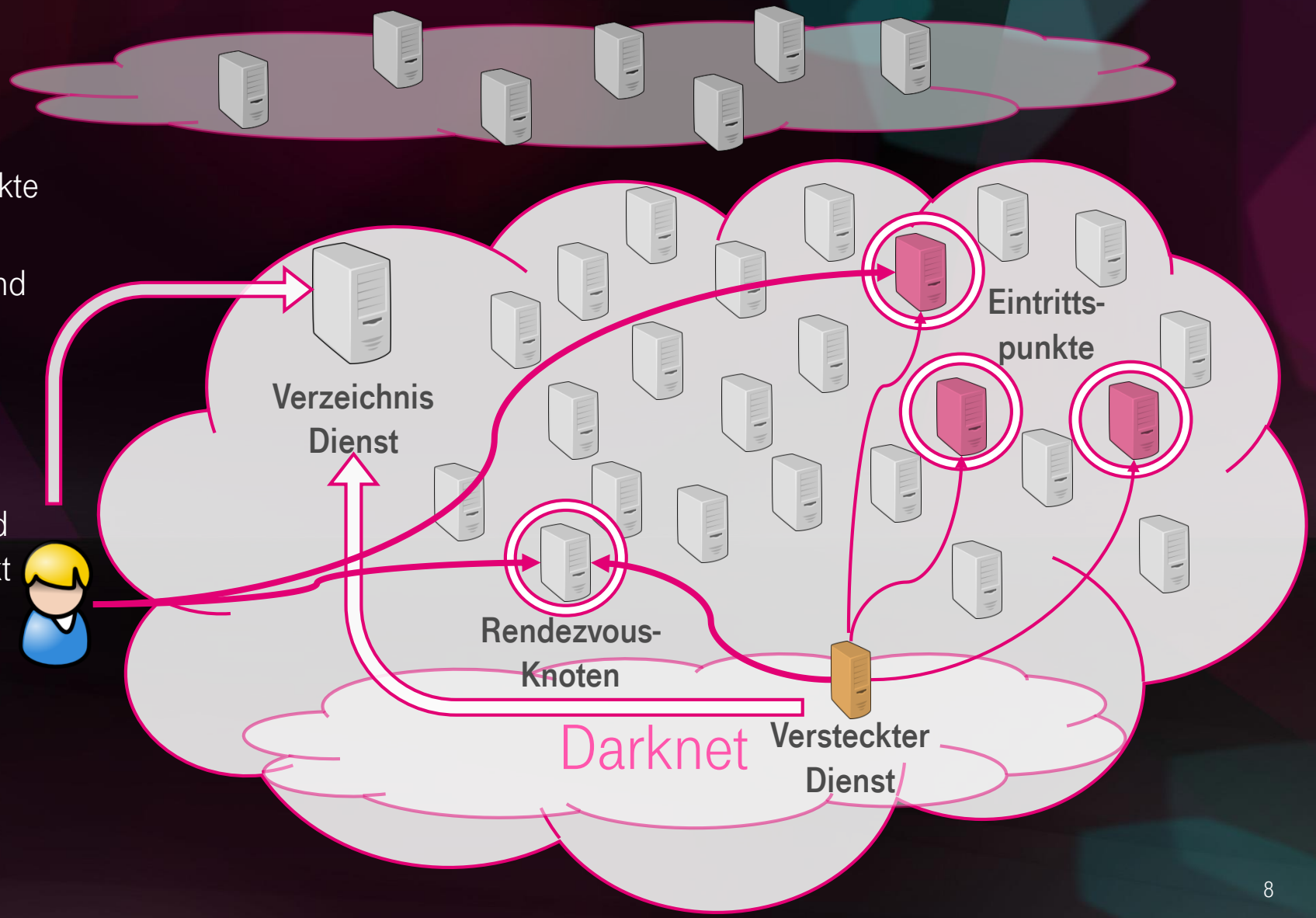
Schnelle Installation

Einfach zu bedienen

Windows XP, Vista, 7, 8, 10; Linux

VERSTECKTE DIENSTE IM DARKNET

1. Versteckter Dienst wählt Eintrittspunkte und verbindet sich mit diesen
2. Dienst lädt öffentlichen Schlüssel und Eintrittspunkte ins Verzeichnis
3. Client findet öffentlichen Schlüssel des Dienstes und Eintrittspunkte im Verzeichnis
4. Client wählt Rendezvous-Knoten und sendet diesen an einen Eintrittspunkt
5. Dienst entscheidet ob er sich zum Rendezvous-Knoten verbindet und anonymen Kommunikationsaufbau abschließt



DEEP WEB, TOR, DARKNET

- Internet Angebote nicht indiziert oder suchbar
- Beidseitig anonyme Kommunikation
- kryptografisch geschützte Inhalte
- versteckte Dienste

Überwachung des Netzes als Ganzes nicht möglich

DARKNET

WAS KANN MAN DAMIT TUN?

Drogen

Cyber Crime

Waffen

vs.

Meinungsfreiheit

Zensurfreiheit

Menschenrechte

CYBER ANGRIFFE IM DARKNET BUCHBAR

BOT-NETZE
&
DENIAL OF SERVICE
ANGRIFFE

DDoS attack	1GB packets: • SYN per day • HTTP GET per day 10GB SYN packets per day DNS server attack DDoS toolkit rental: • One month • Six months • One year • Lifetime	 US$16 US$73 US$161 US$323 US$81 US$161 US$258–323 US$452–484
Botnet	Windows: • With 100 Windows XP bots • With 100 Windows Server 2003/2008 bots DDoS attack: • 100 bots • 300 bots • 800 bots • 2,000 bots	 US$8 US$48 US$95 US$208 US$386 US$596
Traffic	500 IP addresses per day 1,000 IP addresses per day 5,000 IP addresses per day 10,000 IP addresses per day 50,000 IP addresses per day 100,000 IP addresses per day 500,000 IP addresses per day	US$0.26 US$0.42 US$2 US$5 US$38 US$95 US$473

DARKNET – MEHR ALS WAFFEN UND DROGEN

- **Whistleblower** können über das Darknet **anonym** ihre Informationen zuspielen
- **Bürger**, die unter einem Regime mit strenger Internet-/Kommunikationsregulierung leben, können **ohne Zensur** mit der Außenwelt kommunizieren
- **Dissidenten** können trotz Nachrichtenzensur **politisch agieren** (Iran, Ägypten)
- **Nutzer** können sich unzensierter über **soziale Netzwerke** austauschen (Facebook im Darknet: https://facebookcorewwwi.onion/)
- **Auslandskorrespondenten** können **geschützt** über politisch brisante Ereignisse aus unsicheren Ländern **berichten**
- **Informanten** können - von der Gegenseite **unerkannt** - Informationen an Dienste **melden**

DARKNET

WOHER STAMMT DAS?

White Hats

Grey Hats

Black Hats

URSPRÜNGE

Ursprung der Entwicklung

- wissenschaftliches Interesse
- Schutz der Privatsphäre
- Sichere Kommunikation
- Unabhängigkeit von Providern und Dienstanbietern
- Schutz vor Verfolgung

Treiber

- „Nerds“
- Sicherheitsexperten

später

- File Sharer
- Raubkopierer

TOR VON RENOMMIERTEN ORGANISATIONEN GEFÖRDERT

entwickelt ab 2000 von Matej Pfajfar an der University of Cambridge

unterstützt durch

- United States Naval Research Laboratory
- Office of Naval Research
- Defense Advanced Research Projects Agency (DARPA)
- Electronic Frontier Foundation

Finanzierung: 60% US-Regierung / 40% Spenden

2011 **Auszeichnung** für „Social Benefit“ durch Free Software Foundation

seit 2014 **Facebook** im Tor-Netzwerk

DARKNET

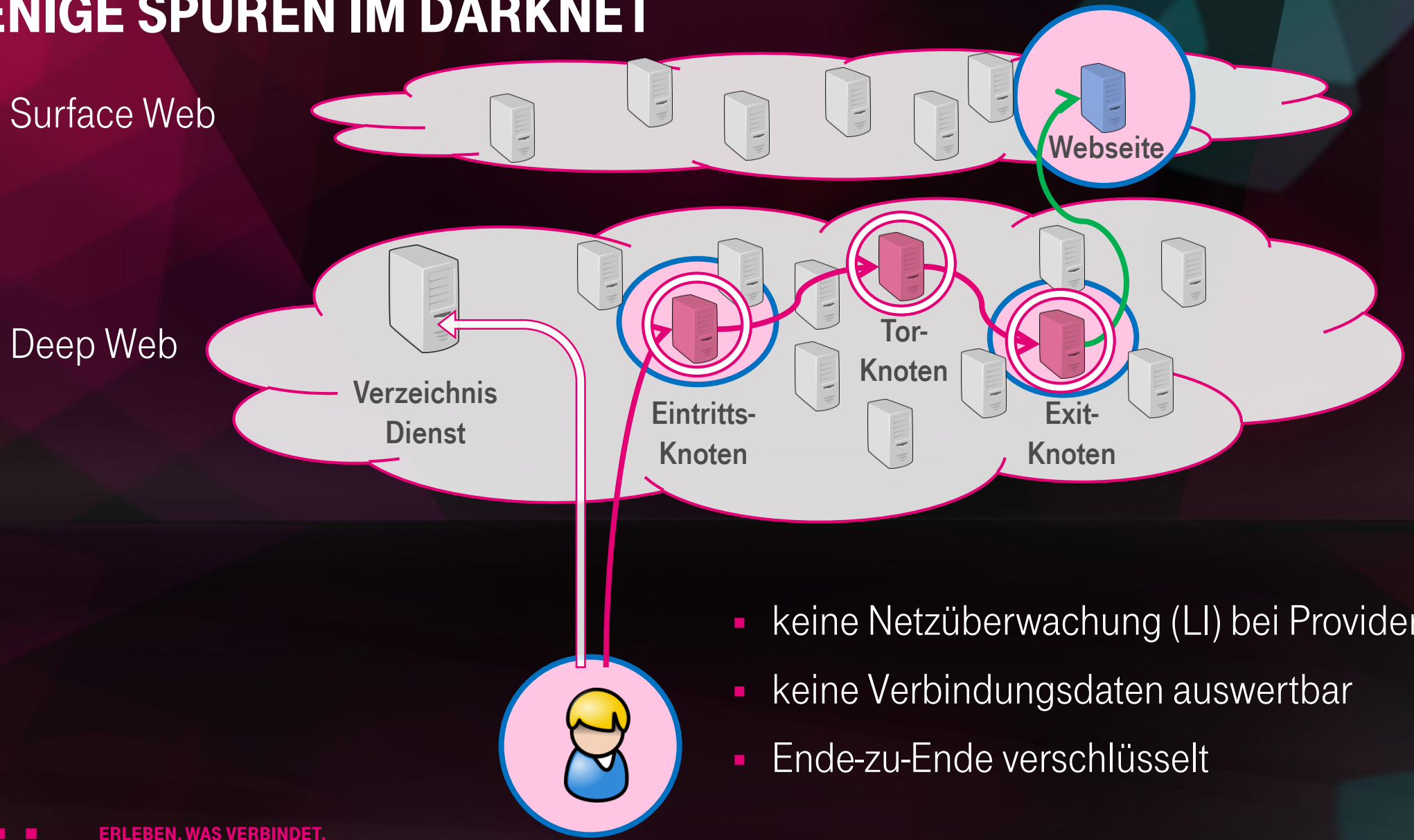
WAS IST KRITISCH DARAN?

neue Kommunikationsstruktur

vs.

klassische Netzüberwachung

WENIGE SPUREN IM DARKNET



- keine Netzüberwachung (LI) bei Provider
- keine Verbindungsdaten auswertbar
- Ende-zu-Ende verschlüsselt

DARKNET IST NICHT DAS ENDE DER STRAFVERFOLGUNG

Verkehrsüberwachung über den „**Netzbetreiber**“ (gibt es im Darknet nicht) nicht möglich!

Ausleiten unmöglich, Auskunftsersuchen erschwert

ABER:

- Darknet ist als Teil das Internets **erreichbar**, wenn man weiß wo
- Einschleusen von **Exit-Nodes** ist bereits Gang und Gäbe
- Überwachung von **Zielpersonen** auf dem **Endgerät** immer möglich, einfacher und notwendig aufgrund Vielzahl verschlüsselter Dienste
- Wechsel in der Taktik erforderlich: **lokale Ermittlung** in Täterkreisen statt technisch im Netz

DARKNET

WIE WOLLEN WIR DAS BEWERTEN?

unbeobachtet sein

reale Welt

vs.

Darknet

DEEP WEB UND DARKNET SIND DIE MODERNEN HINTERZIMMER

klassisch

Schutz des privaten Umfelds
Das „Schlafzimmer“ ist tabu.

Drogendealer hatte bisher auch kein angemeldetes Ladenlokal.

Wir akzeptieren und schätzen das unbeobachtete Vier-Augen-Gespräch – bis hin zu Geheimlogen.

World Wide Web

Nutzer schützen sich vor zu großer Neugier von Web-Diensten.

Kriminelle nutzen unbeobachtete Bereiche im Web.

Legitimer Informationsaustausch wird im Darknet vor Repression geschützt.

WIR BRAUCHEN DEN INFORMIERTEN DISKURS

Das Darknet ist eine wertfreie, technische Kommunikationsplattform
Mit der fortschreitenden Digitalisierung entstehen „Hinterzimmer“ und „dunkle Hauseingänge“ im Web.

Das Darknet kann nicht abgeschaltet oder verboten werden.
Notwendige Ermittlungs- und Überwachungsmaßnahmen müssen der neuen Technik angepasst sein.

Wir müssen die Diskussion darüber **informiert und sachlich** weiterentwickeln:
Nicht „Sicherheit **oder** Freiheit“, sondern „Freiheit **mit** Sicherheit“.

FRAGEN?
FRAGEN!

Weitere Informationen

- How Tor Works: https://youtu.be/LAcGiLL4OZU
- What data is visible to whom: https://www.eff.org/pages/tor-and-https
- Deep Web: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104