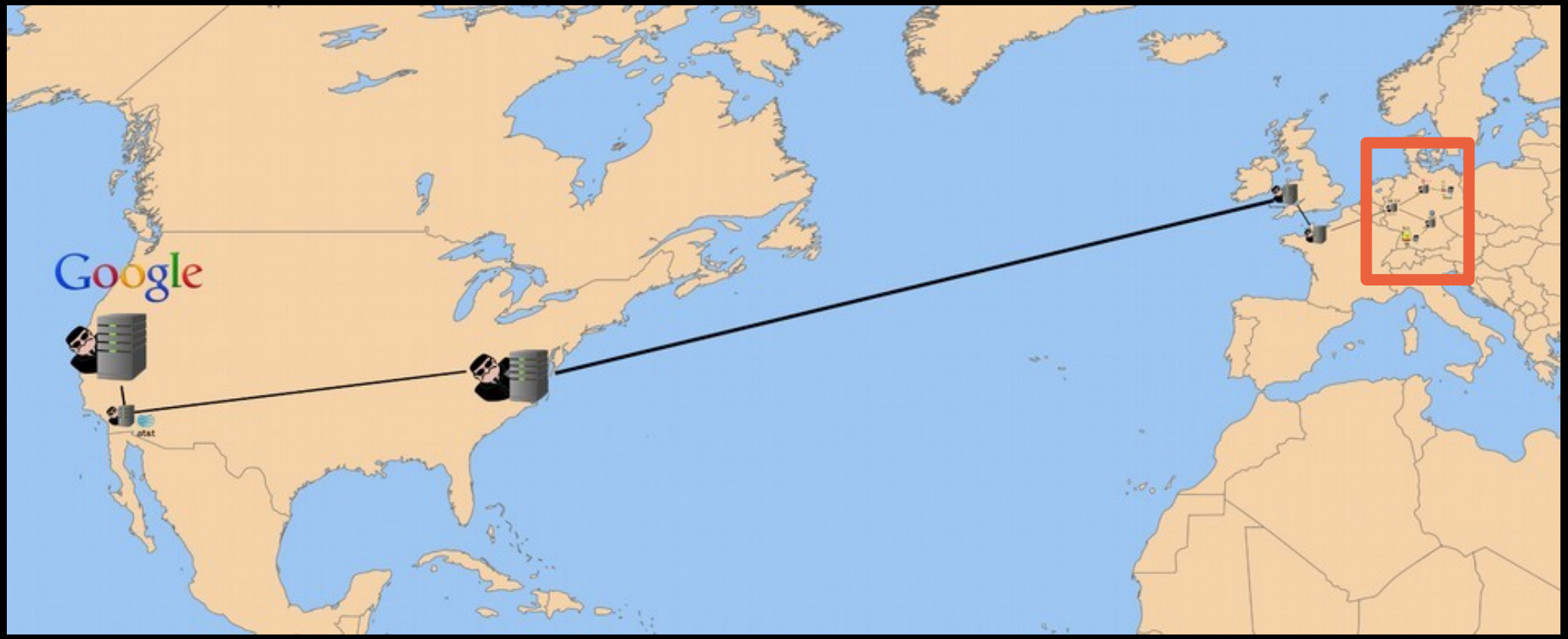
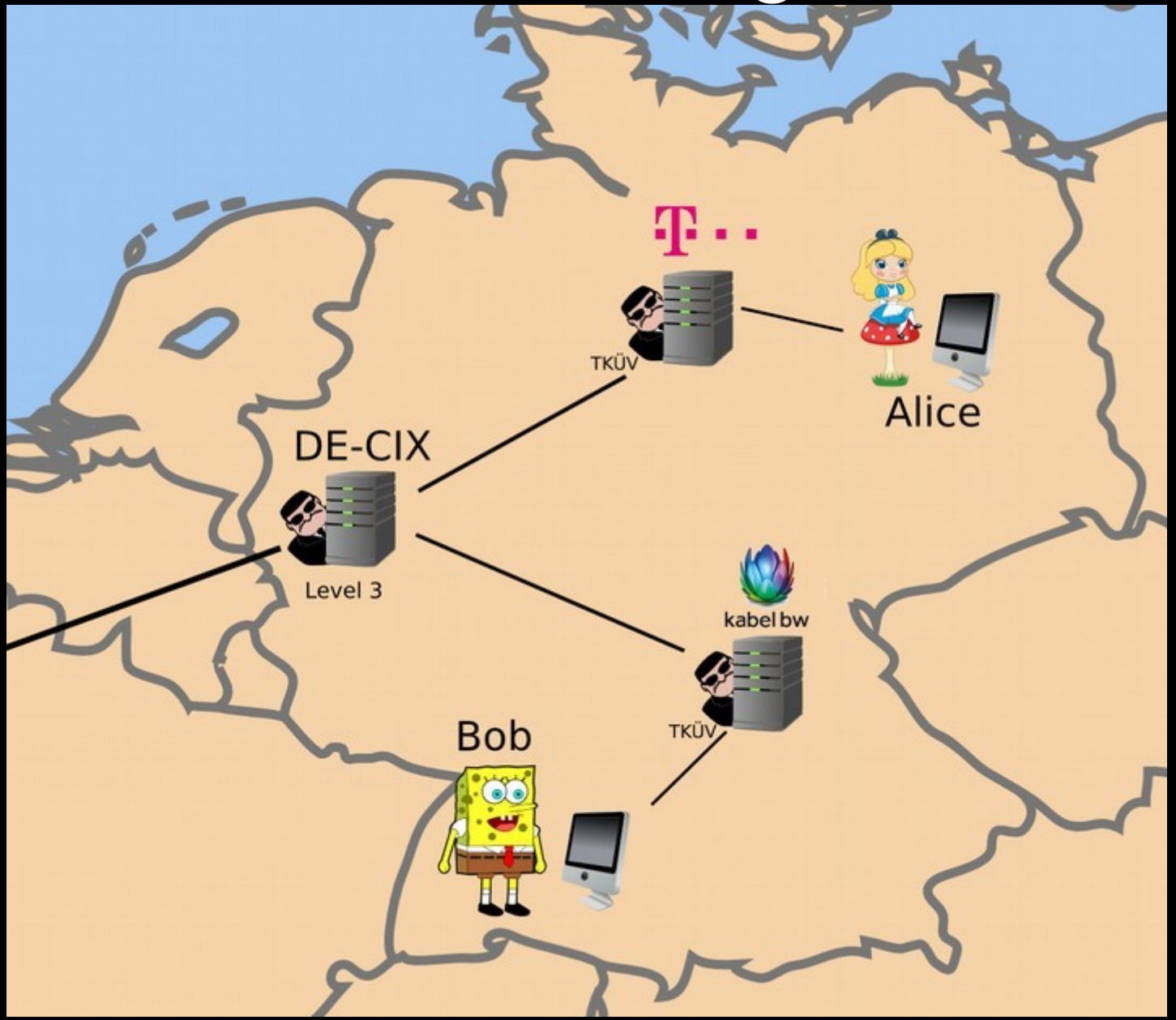
Prism, Tempora und Co. - Wie wir überwacht werden und wie wir uns verteidigen können

Referent:
Stefan Leibfarth

Überwachung am Beispiel einer E-Mail über „Google Mail“



Überwachung am Beispiel einer E-Mail über „Google Mail“



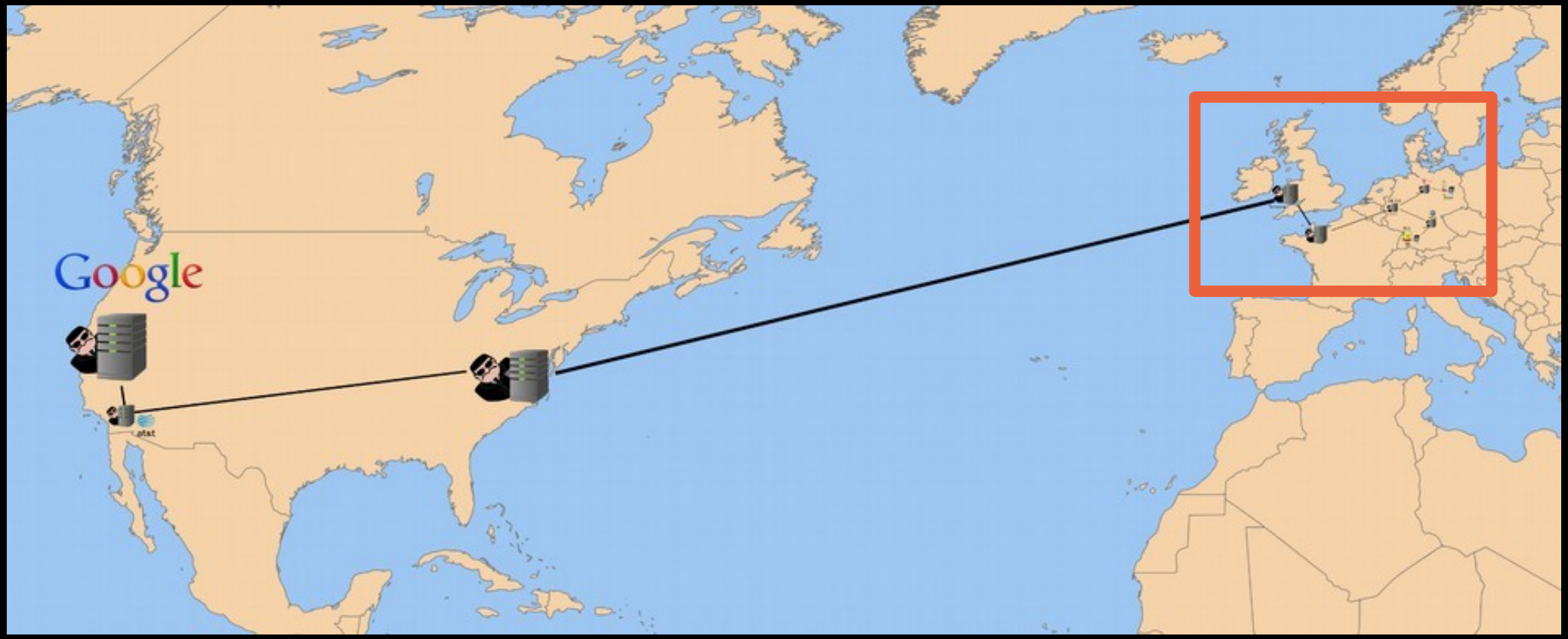
Abhören am DE-CIX

- Datenweitergabe durch den Netzbetreiber „Level 3“ an die NSA
- Maximal 20% des internationalen Verkehrs durch den BND

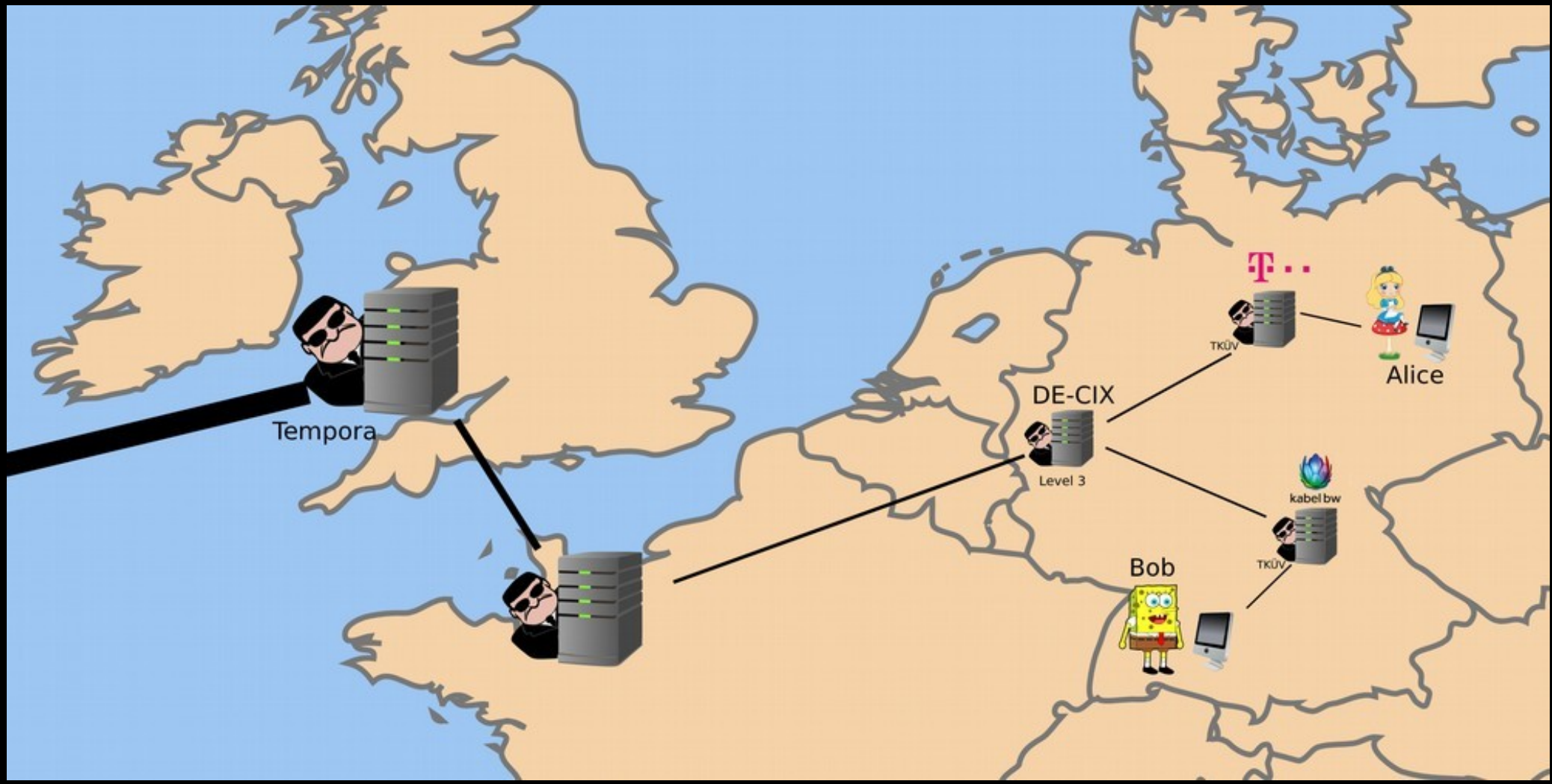
Zusammenarbeit BND ↔ NSA

- Weitergabe von Verbindungsdaten an die NSA (Telefon, E-Mail, SMS, Chat, …)
- Ca. 500 Millionen Datensätze im Monat
- Ausgenommen sind Deutsch (erkennbar an .de-Domain oder +49-Vorwahl)

Überwachung am Beispiel einer E-Mail über „Google Mail“



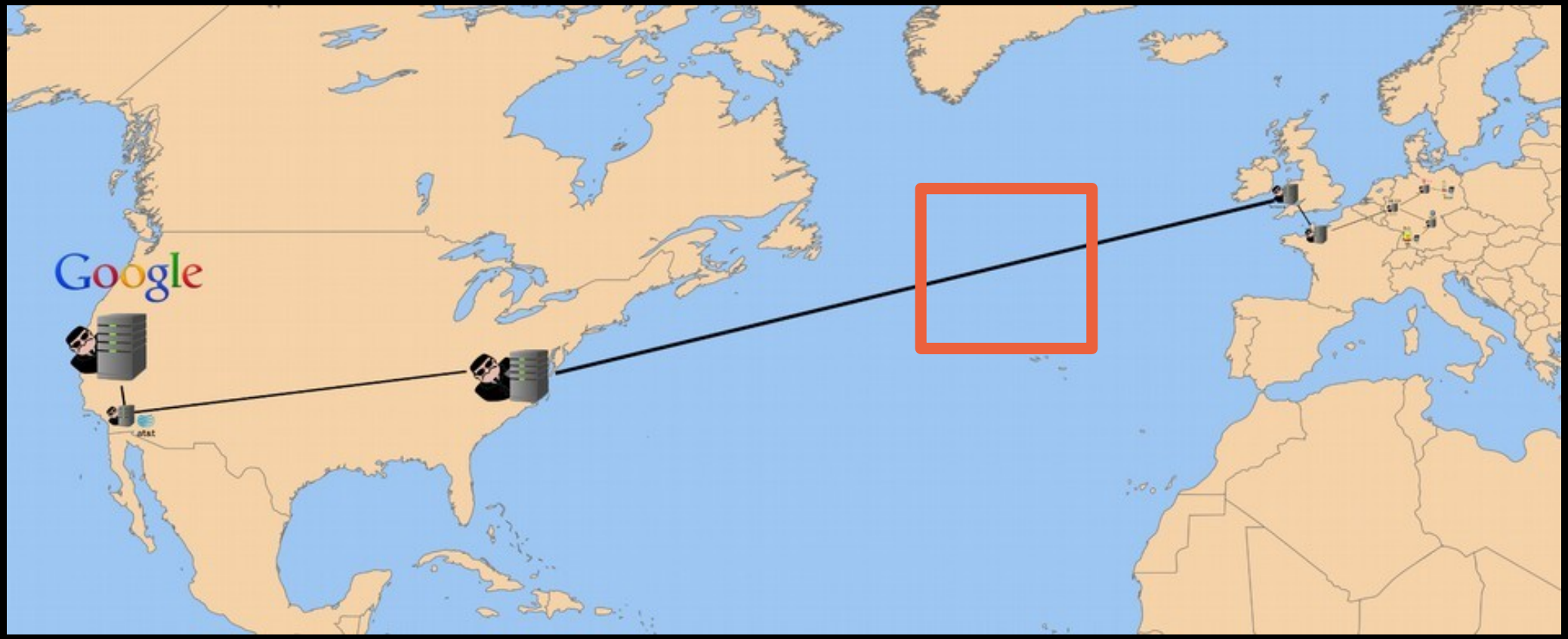
Überwachung am Beispiel einer E-Mail über „Google Mail“



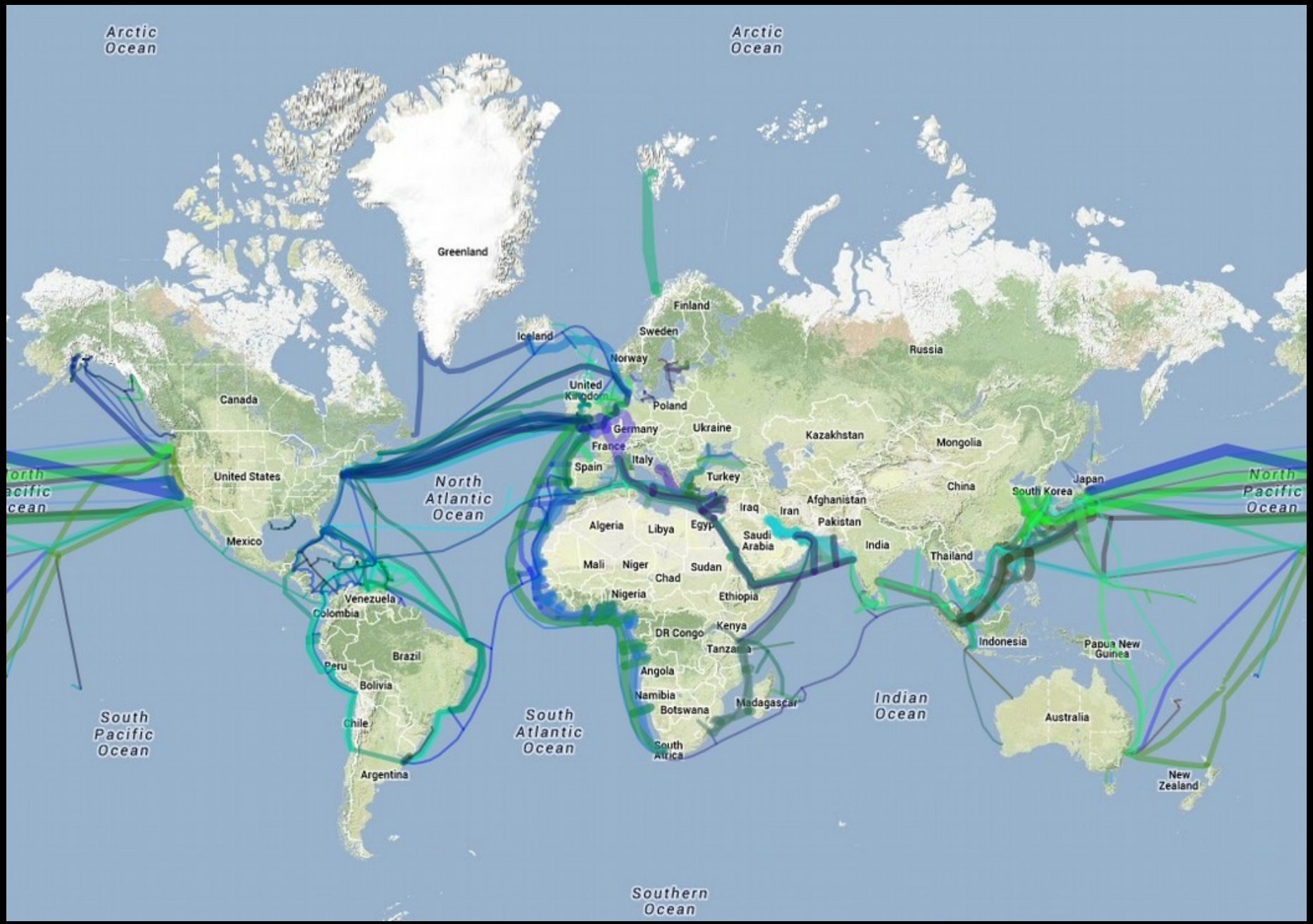
Tempora

- Abhören aller ca. 200 Glasfaserkabel die über UK laufen
- 21 Petabyte am Tag
- Bis zu 3 Tage komplette Speicherung
- Weitergabe der Daten an die NSA
- (Mit)finanziert durch die NSA

Überwachung am Beispiel einer E-Mail über „Google Mail“

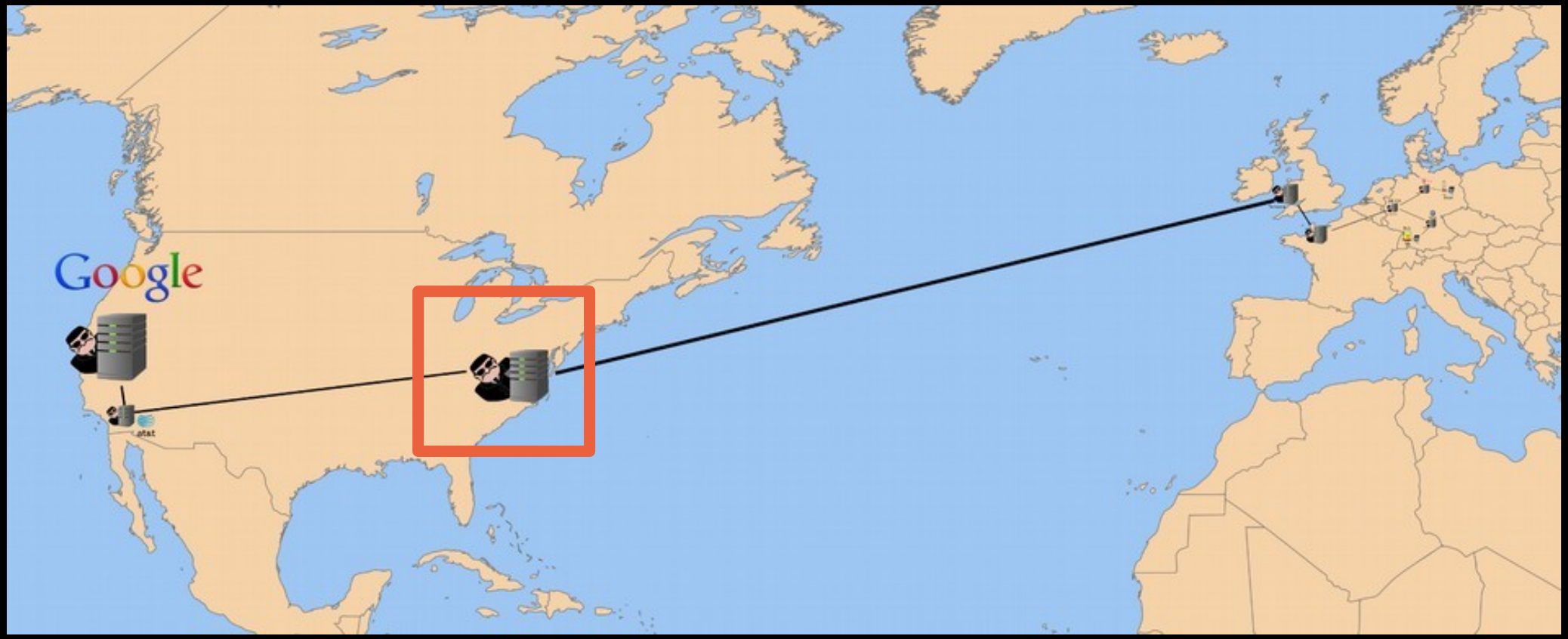


Anzapfen von Seekabeln



Anzapfen von Seekabeln

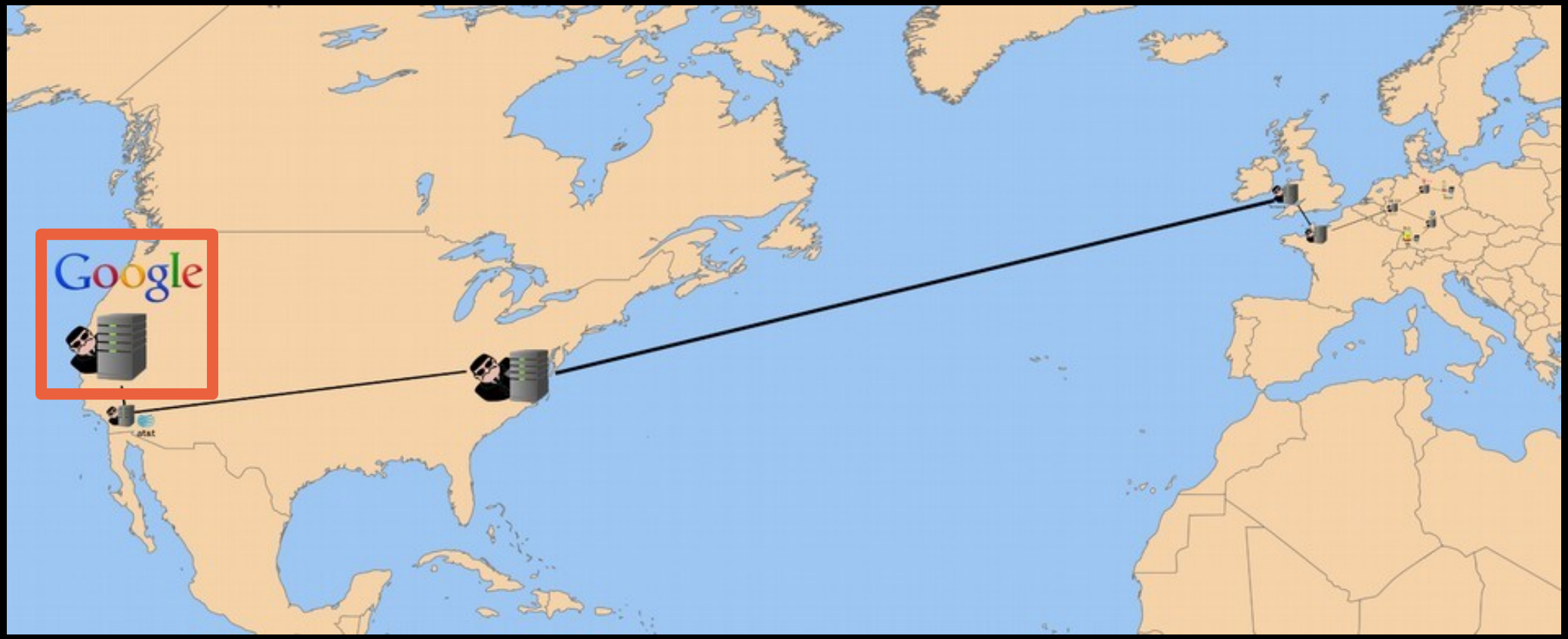
Überwachung am Beispiel einer E-Mail über „Google Mail“



Upstream

- US Gegenstück zu „Tempora“
- Der Großteil des weltweiten Datenverkehrs läuft über die USA

Überwachung am Beispiel einer E-Mail über „Google Mail“




PRISM
Microsoft
YouTube
facebook
Google
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
YAHOO!
skype
Aol.

Wie viel wird gespeichert?

Beispiel: Utah Data Center der NSA

- 1,5 Milliarden $; 90.000m²
- ca. 5 Zettabyte Speicherplatz
  (= 1000 x 1000 x 1000 Terabyte)
- ein Ziel: im Jahre 2018 256-bit AES brechen
- Visualisierung für unseren Bundespräsidenten

Was wird mit den Daten gemacht?

- Digitaler Doppelgänger
- X-Keyscore

  Echtzeitsuche und Überwachung z.B. „Alle Anführer der Bewegung gegen Stuttgart21“
- Drohnen-Morde
- Wirtschafts-Spionage

Wie bin ich betroffen?

- Jeder ist verdächtig (anlasslose Überwachung)
- Konsequenzen nicht absehbar (Erpressbarkeit, Verfolgung, …)
- Selbstbeschränkung

Grundgesetz-Verletzung

Was sollte unsere Regierung tun?

Forderungen des Aktionsbündnisses

„Stop Watchin Us“

- vollständige Aufarbeitung der Vollüberwachung
- Schluss mit Massenüberwachung
- Snowden aufnehmen
- keine Vorratsdatenspeicherung
- keine Bestandsdatenauskunft

Was sollte unsere Regierung tun?

Darüber hinaus fordert der CCC

- Strafverfolgung der der Beteiligten
- Abschaffung der Geheimdienste
- Auflösung des "Safe Harbor"-Abkommens
- Maßnahmen zur zukünftigen Sicherung der Rechtsstaatlichkeit
- Politischen Druck auf die US und UK Regierung, die Datenschutzbestimmungen europäischer Länder zu achten

Was kann jeder Einzelne tun?

politisch / gesellschaftlich

- Das Problem ansprechen
- Die richtige Partei wählen
- Demonstrieren gehen
- Mit Abgeordneten reden

Was kann jeder Einzelne tun?

technisch

- FOSS
- Datensparsamkeit
- Dezentrale Systeme
- Raus aus der „Cloud“
- US-basierte Anbieter meiden
- Verschlüsselung (Welche ist noch sicher?)

Betriebssystem

Jede Software ist nur so sicher und vertrauenswürdig, wie das Betriebssystem auf dem sie läuft.

→ LINUX

Für Einsteiger empfehlenswert:

E-Mail Verschlüsselung
mit PGP

Was bringt das?

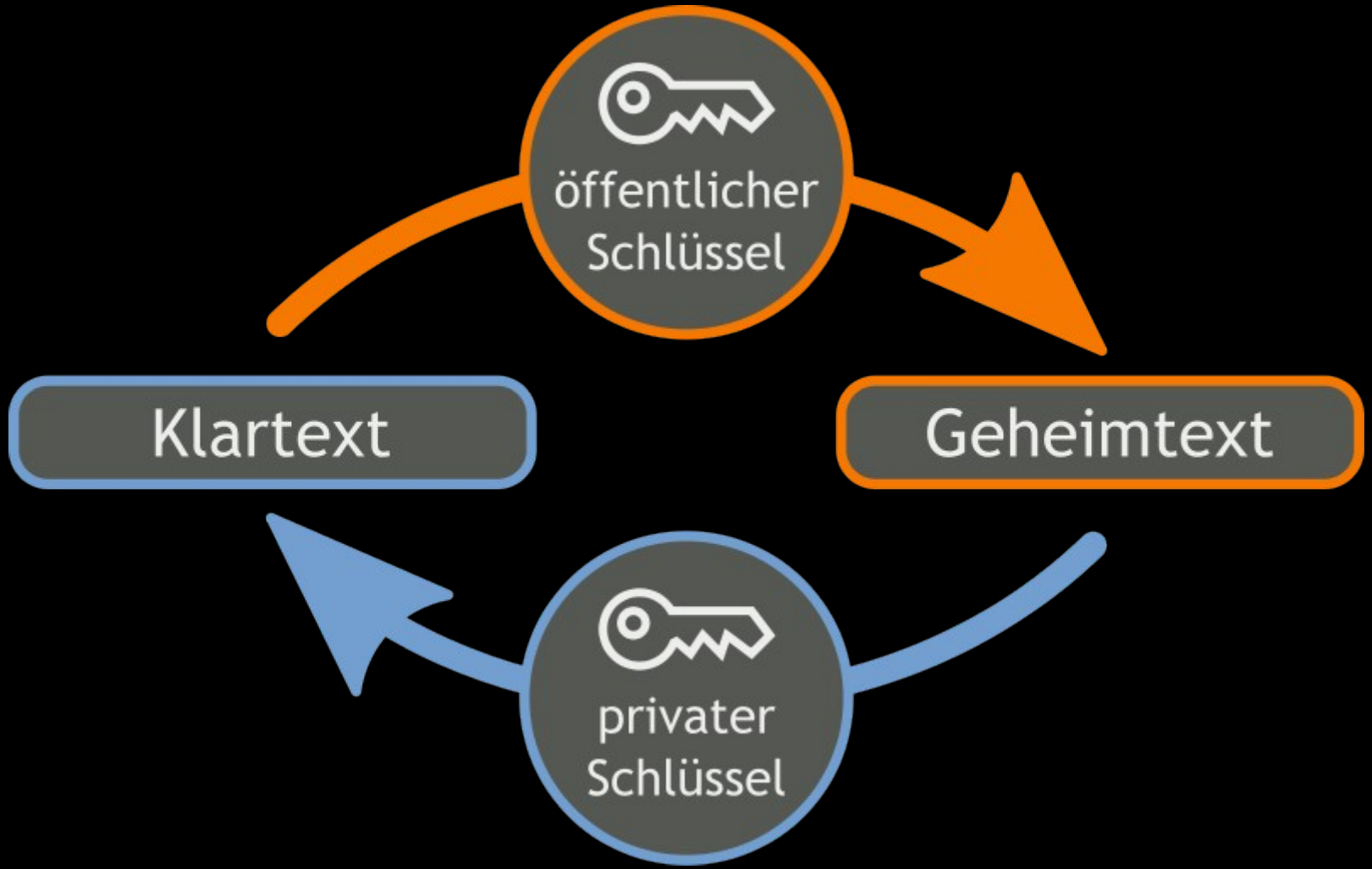
Inhalt der Mail bleibt Dritten verborgen (Nicht der Betreff und nicht die Verbindungsdaten!)

<u>Bonus:</u>

- Absender kann überprüft werden
- Veränderungen an der Mail können ausgeschlossen werden

E-Mail Verschlüsselung

Hier: Asymmetrische Verschlüsselung



E-Mail Verschlüsselung

Offene Fragen:

- Woher bekomme ich den öffentlichen Schlüssel meines Kontakts?
- Woher weiß ich, dass ich den Richtigen habe?

E-Mail Verschlüsselung

Voraussetzungen:

- Thunderbird installiert und vorhandenes Mail-Konto eingerichtet
- Das Plug-In „Enigmail“ in Thunderbird installiert
- Windows benötigt zusätzlich „Gpg4Win“ / OSX benötigt „PGPTools“

Los geht’s! (Ausführliche Anleitung)

Tipp: Sicheres Passwort (englisch)

E-Mail Verschlüsselung

… ist auch auf dem Smartphone möglich

- Android
  - K-9 Mail als Mail-Client (wie Thunderbird)
  - APG für die Verschlüsselung (wie Enigmail)
- iOS
  - IPGPMail

Wichtig: Gerät verschlüsseln um bei Verlust auf der sicheren Seite zu sein. (Tipp zu Android)

Off-the-record messaging

- Verschlüsselung für XMPP-Chats (z.B. auch Facebook, Gtalk, …)
- Für Desktop (z.B. Pidgin + OTR-Plugin) und Smartphone (Gibberbot)
- Kein „festen“ Schlüssel wie bei PGP
- Fingerabdruck abgleichen!

Anleitung

- Tool zum anonymen surfen
- Statt direkter Verbindung werden 3 Server zwischen geschaltet
- „Tor Browser Bundle“ zum sofort los legen

Erweiterung für Firefox

DuckDuckGo

Suchmaschine, die keine Anfragen speichert

- Alternatives Android
- Ohne proprietäre Google Dienste
- „Free Your Android“
- F-Droid als Quelle für FOSS Apps

Prism-break.org

Sammlung von weiteren, freien Alternativen zu bekannten proprietären Programmen und Services

Kontakt

- E-Mail: stefan@leibfarth.org

  Fingerabdruck: F8FC B504 087A C78B 1462

  7894 E5CE BB2A C135 4426
- XMPP: stefan@leibfarth.org
- Twitter: @leibi_

Fragen?

Quellen

- CCCS Logo: CCCS e.V. CC by-nc-sa
- Linux Mint Logo: Clement Lefebvre CC BY 3.0
- Prism Logo: NSA, US government; prism photograph: Adam Hart-Davis © 1998-04-08
- Mircosoft Logo: Microsoft Corporation
- Google Logo: Google Inc.
- NSA Logo: U.S. Government
- Yahoo Logo: Yahoo
- Facebook Logo: facebook.com website - [Designed by Cuban Council. Based on modified "Klavika" font.]
- Youtube Logo: Youtube
- Karte der Internet-Kabel: cablemap.info und Google Maps
- Tor Logo: Torpoject.org
- USS Jimmy Carter: U.S. Navy photo Photographer's Mate 2nd Class George Trian (RELEASED)