

Edward Snowdens Koffer

Was die Geheimdienste eigentlich mit Ihren Daten
anfangen wollen und wie Sie das verhindern

Ben Hermann

 @benhermann

6. Juni 2013

US national security

Glenn Greenwald on
security and liberty

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama

- [Read the Verizon court order in full here](#)
- [Obama administration justifies surveillance](#)

Glenn Greenwald

Thursday 6 June 2013 11.05 BST



theguardian

11. Juni 2013



theguardian

Was ist da passiert?



Mit dabei sind ca. 1,7 Millionen Dateien

Was ist im Koffer?

- Formate
 - Präsentationen
 - Dokumentationen
 - Protokolle
- Quellen
 - National Security Agency (NSA)
 - Department of Defence (DoD)
 - Australian Intelligence Community (AIC)
 - Geheimdienste des Vereinigten Königreichs (meist GCHQ)
- 1,7 Millionen Dateien mitgenommen, jedoch nur ca. 10.000 weitergegeben

Einen Schritt zurück

Wer ich bin....

Dipl.-Inform. Ben Hermann
Doktorand an der TU Darmstadt

Forschung zu analytischer und
konstruktiver Sicherheit für
Software



 @benhermann

www.thewhitespace.de

Viele zu viele Filme und Bücher
zu Spionagethemen konsumiert

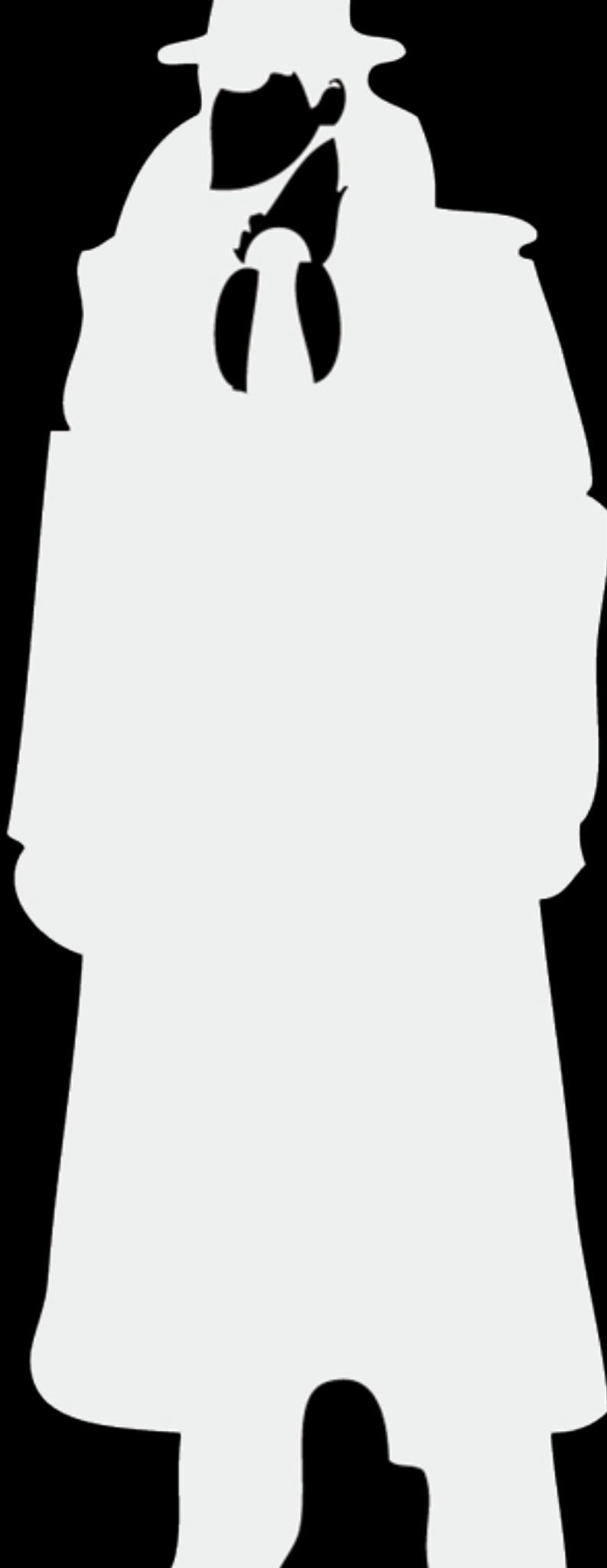
Worüber ich heute sprechen werde...

Warum gibt es Geheimdienste?

Auf welcher Grundlage arbeiten Geheimdienste?

Was sammeln unsere Geheimdienste und was
wollen sie damit?

Wie können Sie sich dagegen schützen?



Warum gibt es
Geheimdienste?

Geschichte

- Spionage ist so alt wie die Menschheit
- Geheimdienste im heutigen Sinn sind im zweiten Weltkrieg entstanden
- Militärischer Erfolg war zunehmend vom Informationsstand abhängig

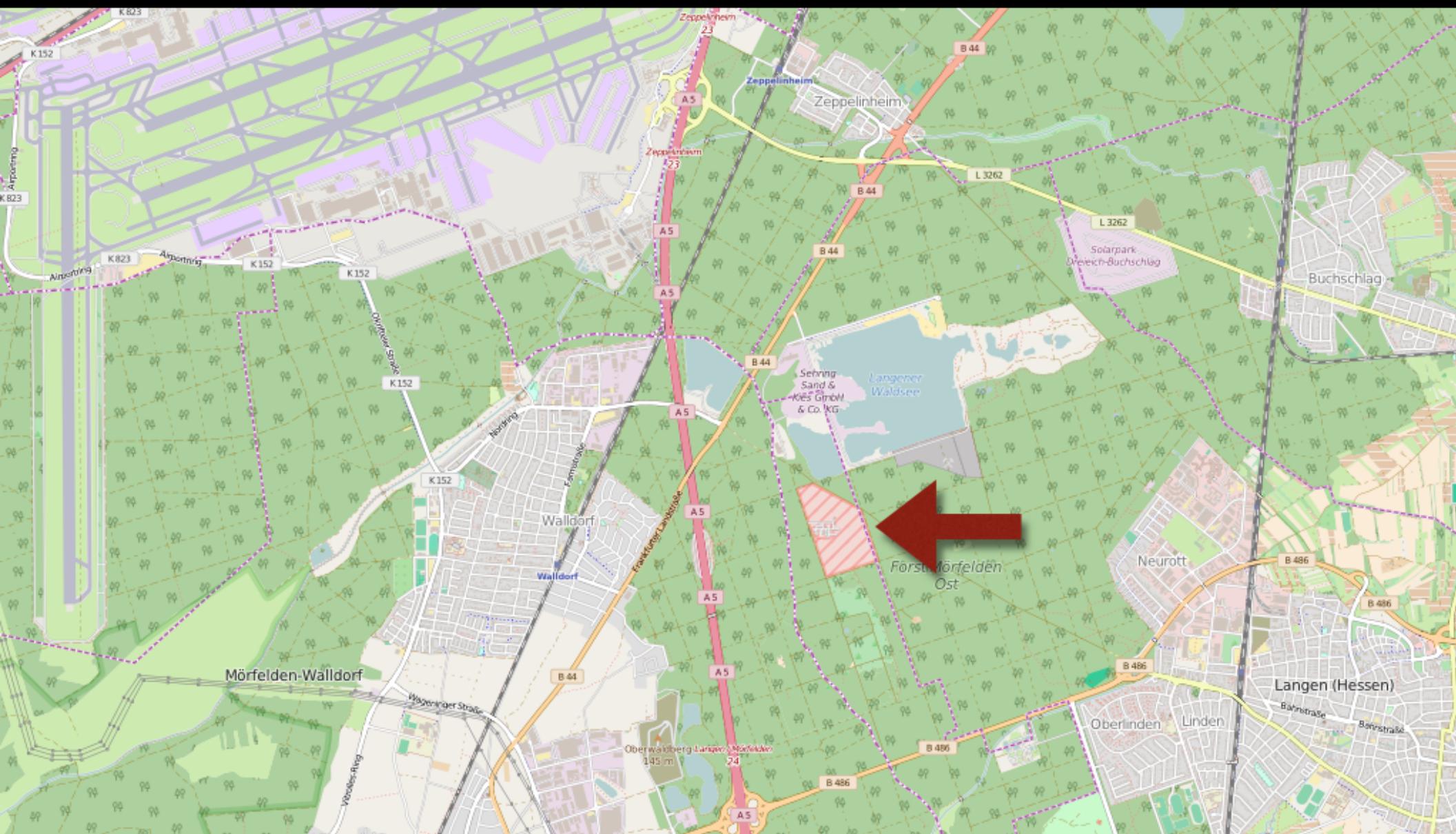




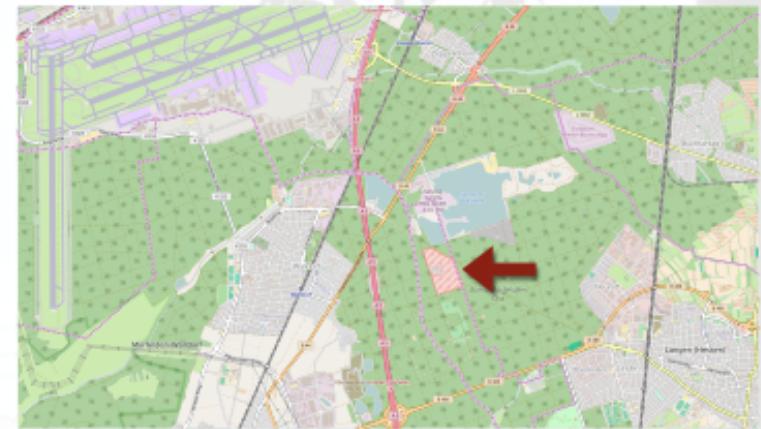
Aufgaben eines Geheimdienstes

- Gewinnung von Erkenntnissen über das Ausland, die von außen-, sicherheits- und militärpolitischer Bedeutung sind.
- Gewinnung von wirtschaftlichen Erkenntnissen
- Abwehr von geheimdienstlicher Aktivität einer fremden Macht
- Sammlung und Auswertung von Informationen über Bestrebungen, die gegen den Bestand oder die Sicherheit des Staates gerichtet sind
- Sicherheitsüberprüfung von Personen
- Technische Sicherungsmaßnahmen (z.B. Fernmeldeverkehr)

Auf welcher Grundlage
arbeiten Geheimdienste?



Egelsbach Transmitter Facility

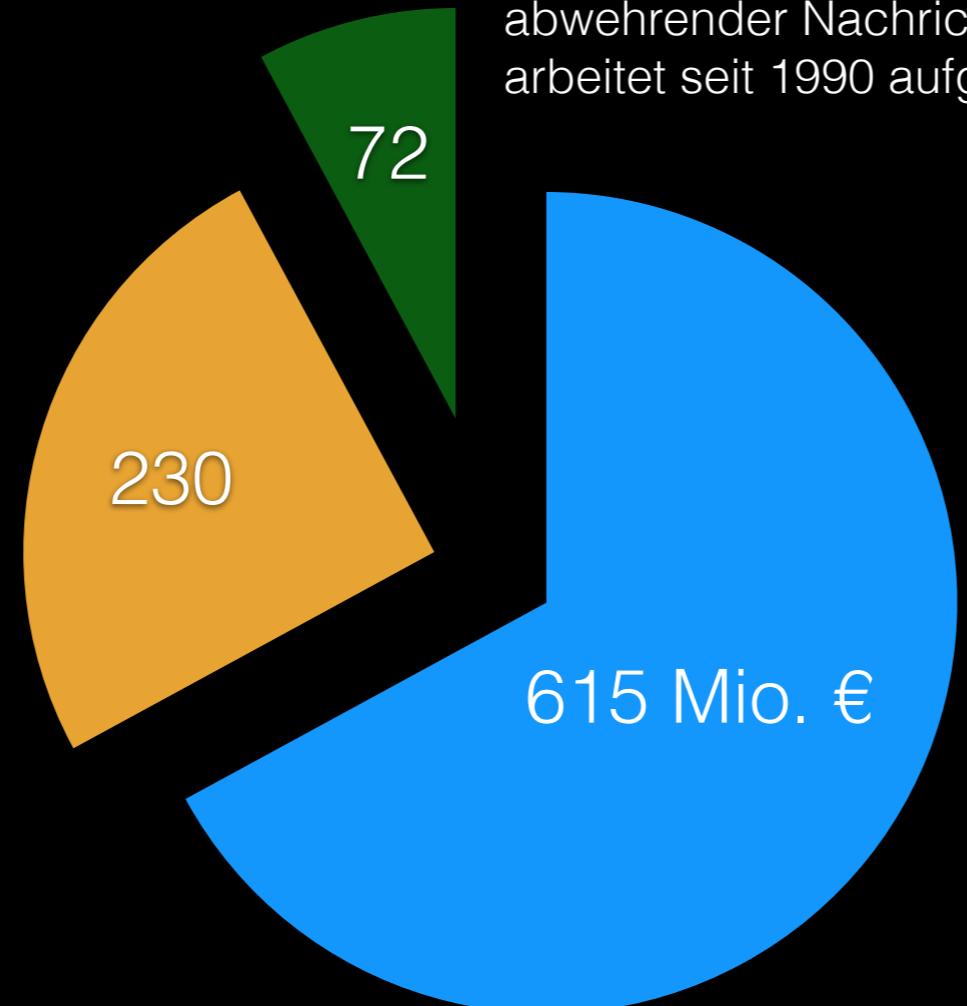


Fernmeldeaufklärungsstation der USA

Bis 2003 Zahlensender E05 Cynthia

2011 nochmals stark ausgebaut

Deutschland



Bundesamt für
Verfassungsschutz
(BfV)

Schutz der freiheitlich
demokratischen Grundordnung
(innere Sicherheit)
arbeitet seit 1950 aufgrund des
Bundesverfassungsschutzgesetzes

Militärischer Abschirmdienst (MAD)
abwehrender Nachrichtendienst
arbeitet seit 1990 aufgrund des MAD-Gesetzes

Bundesnachrichtendienst (BND)
Auslandsaufklärung
arbeitet seit 1990 aufgrund des BND-Gesetzes

Gesetzliche Dualität

BND-Gesetz
§1 Satz 2

Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus.

Strafgesetzbuch
§99 Geheimdienstliche Agententätigkeit

- (1) Wer
1. für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist, oder
 2. gegenüber dem Geheimdienst einer fremden Macht oder einem seiner Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt,
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft [...]



National Security Agency

Aufgabe:

Globale Sammlung und Verarbeitung von Daten (SIGINT)
Schutz der Systeme der amerikanischen Verwaltung und Regierung

Budget:
Geheim

Ursprung im ersten und zweiten Weltkrieg
offiziell gegründet 1952

Arbeitet auf Basis des Foreign Intelligence Surveillance Act von 1978

**UNITING AND STRENGTHENING AMERICA BY
PROVIDING APPROPRIATE TOOLS REQUIRED
TO INTERCEPT AND OBSTRUCT TERRORISM
(USA PATRIOT ACT) ACT OF 2001**



Central Intelligence Agency

Aufgabe:

Sammlung, Verarbeitung und Analyse von Informationen von nationaler Sicherheit durch menschliche Quellen (HUMINT)
Terrorismusabwehr, Waffenkontrolle, Spionageabwehr, Cyberspionage

Budget:
Geheim

Gegründet 1947, nach Pearl Harbor

\$52,7 Milliarden



\$14,7 Mrd.



\$10,8 Mrd.



\$10,3 Mrd.

Quelle: FY 2013 Congressional Budget Justification, The Washington Post 29.08.2013



National Reconnaissance Office

Aufgabe:

Design, Konstruktion und Betrieb von Aufklärungssatelliten
Arbeitet besonders NSA, NGA und DIA zu.

Aufgabe der Satelliten:

Optische und Radaraufnahmen

Kommunikationsrelays

Marineüberwachung

Kommunikationsüberwachung

mind. 30 aktive Satelliten aktuell im Orbit

Gegründet 1961



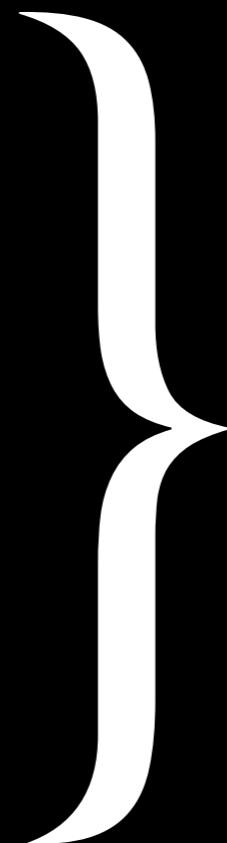
Großbritannien



| SECURITY SERVICE
MI5



SECRET
INTELLIGENCE
SERVICE MI6



£1,8 Mrd.

Quelle: SIA funding website

Frankreich



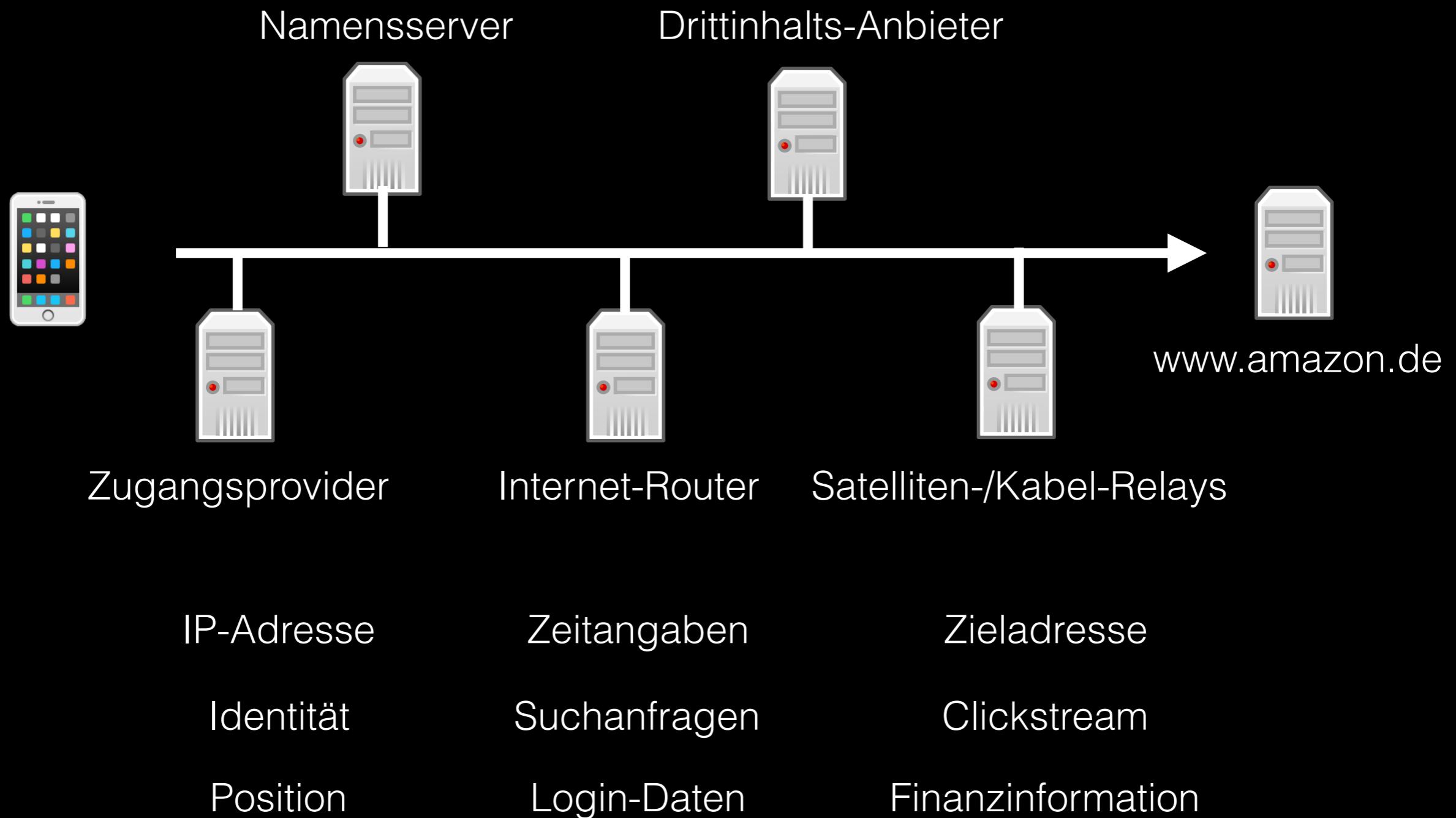
Direction Générale de la Sécurité Extérieure (DGSE)
Budget: 592,8 Mio. €
Spionage und Gegenspionage

HUMINT
SIGINT
Satellitenaufklärung
Special Ops

Aktuell sehr spannende Aktivitäten im
Zusammenhang mit der Verfassungsänderung

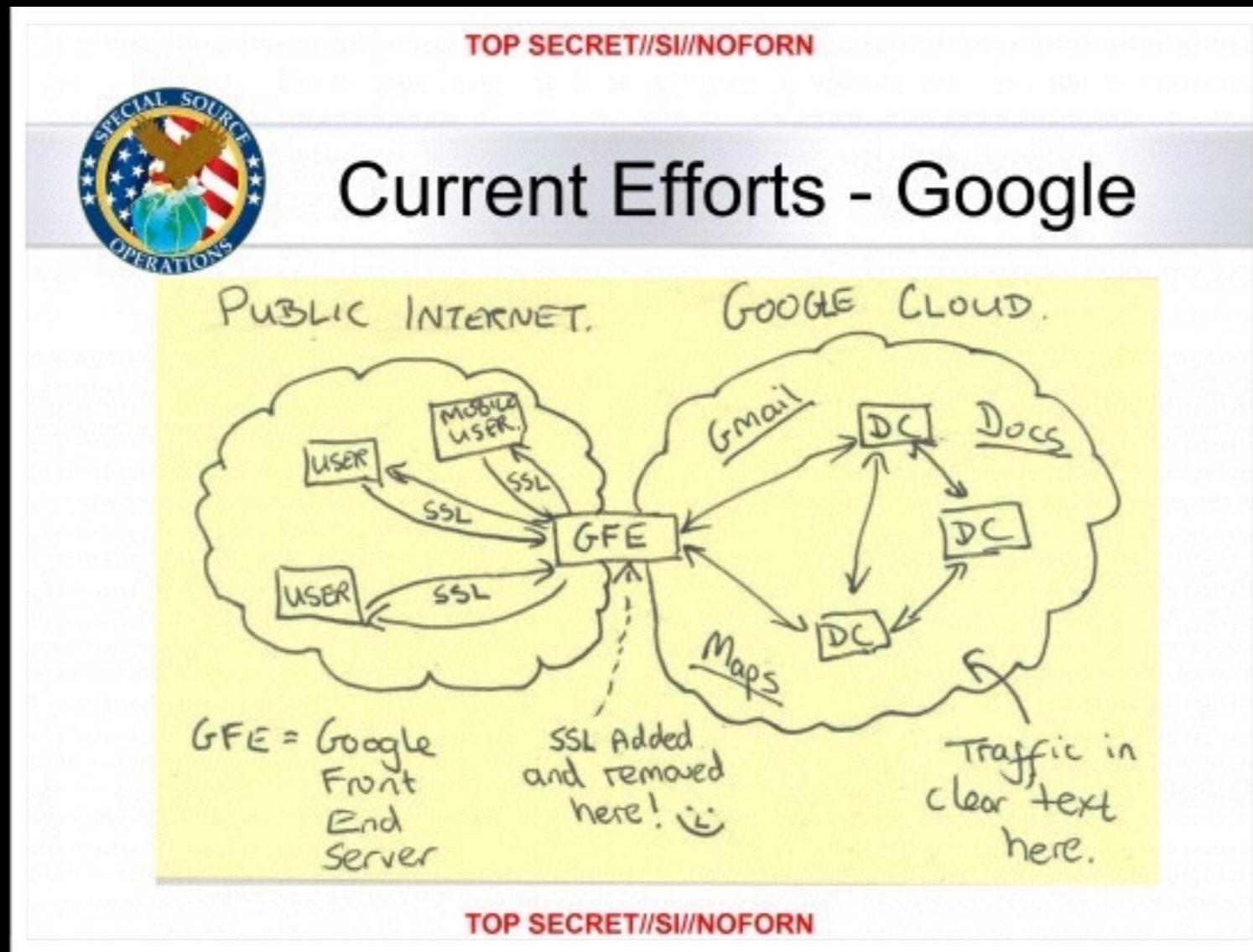
Was sammeln unsere
Geheimdienste und was
wollen sie damit?

Welche Spuren hinterlassen wir im Internet?



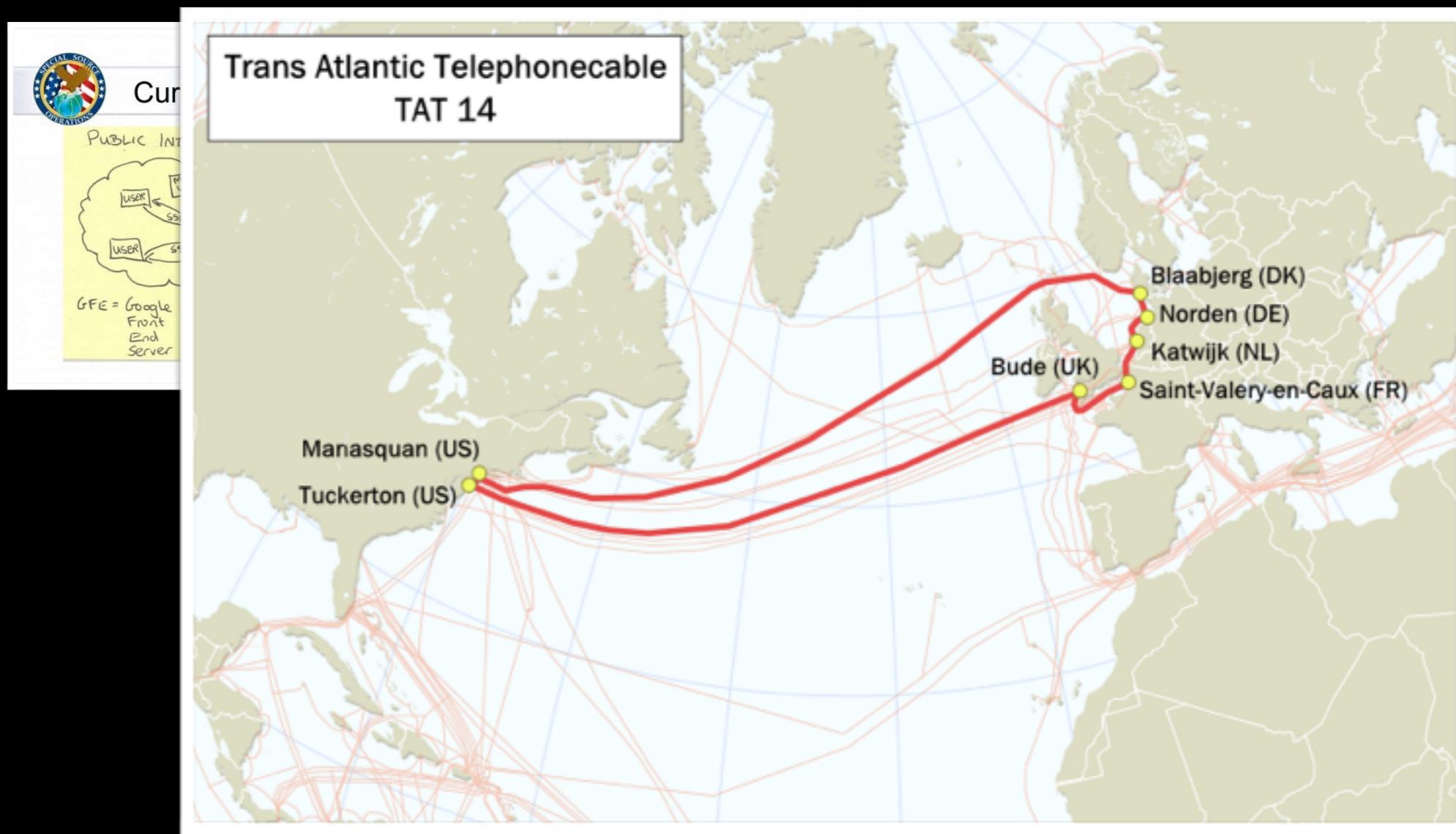
Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



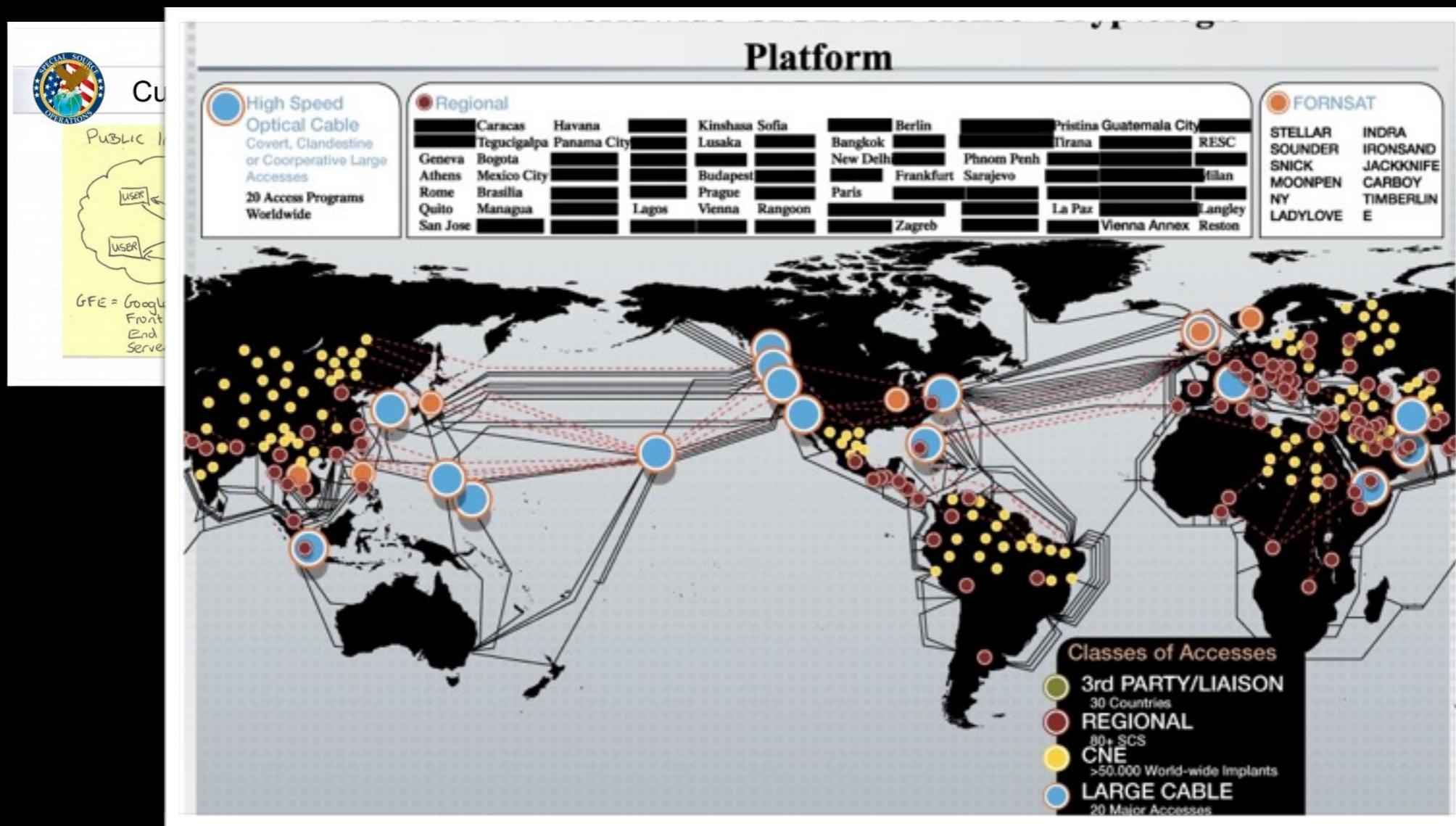
Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



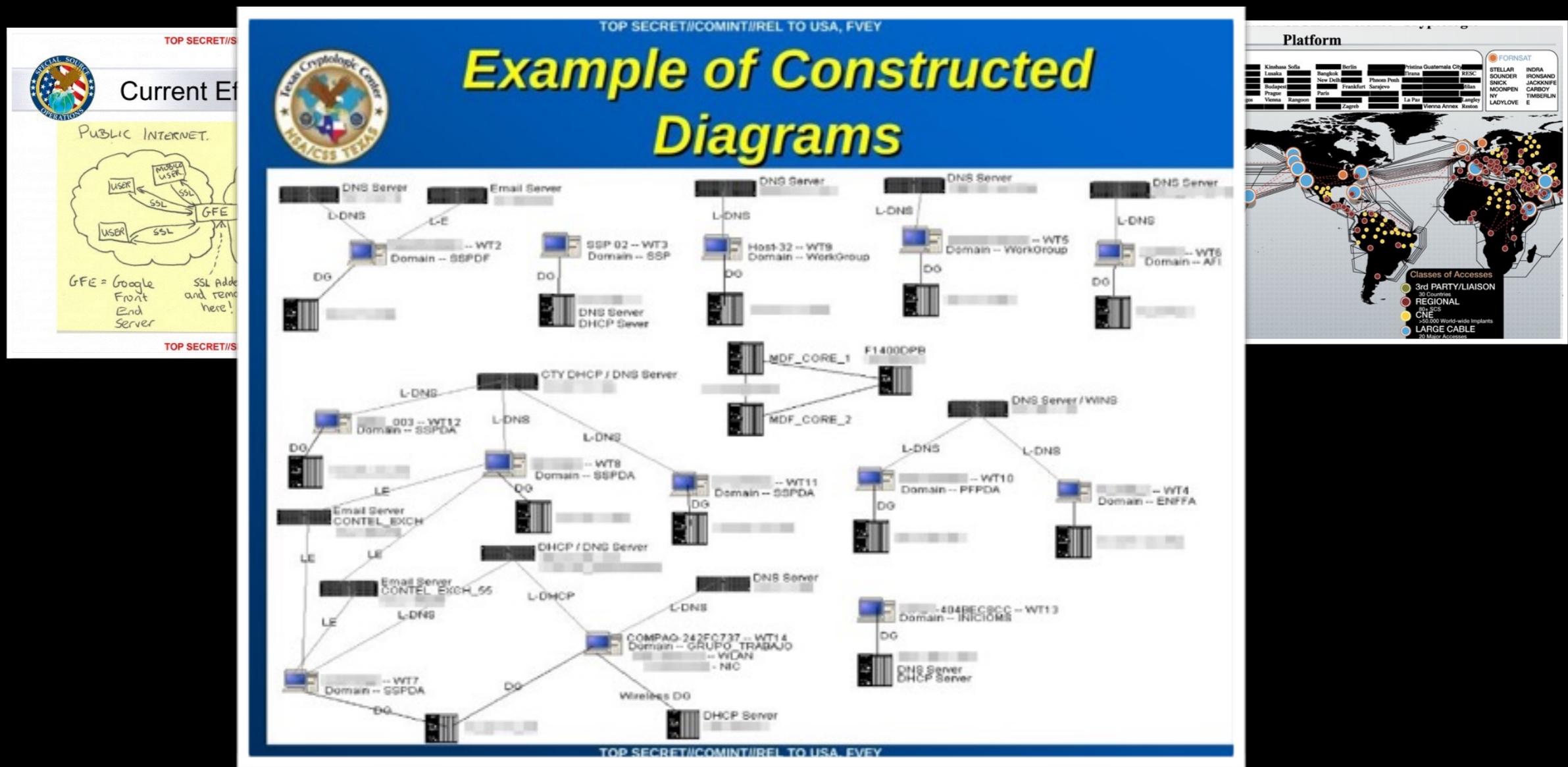
Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



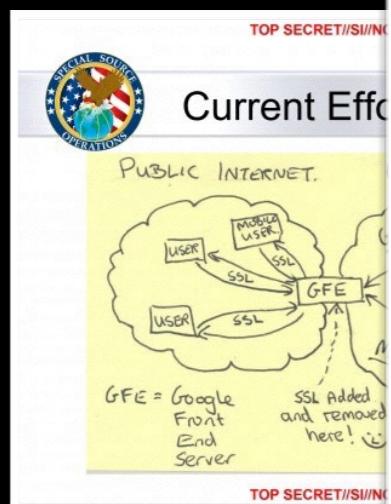
Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



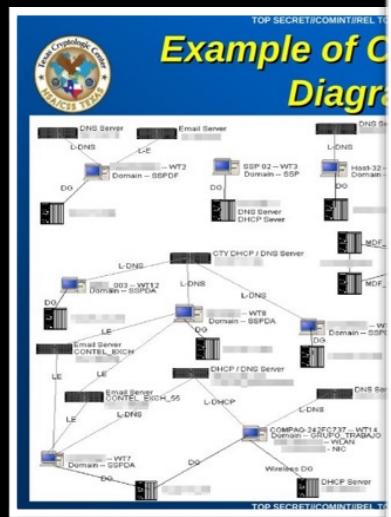
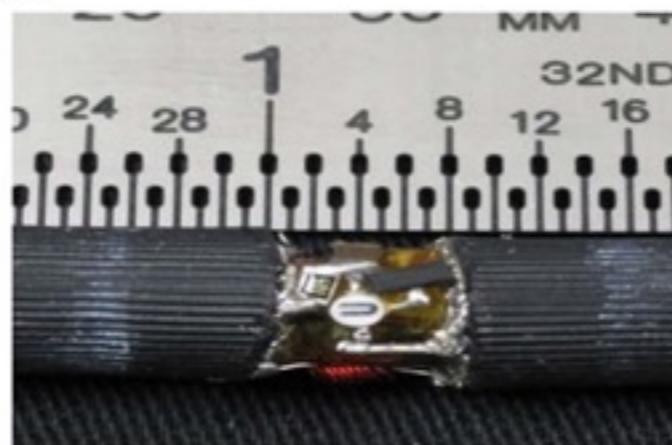
RAGEMASTER ANT Product Data

24 Jul 2008

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

(U) Capabilities

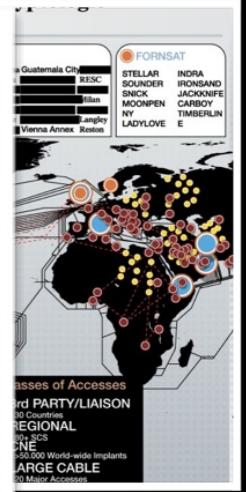
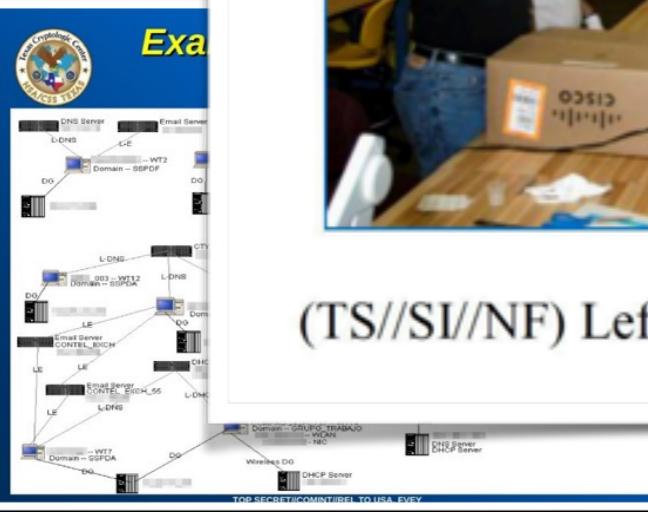
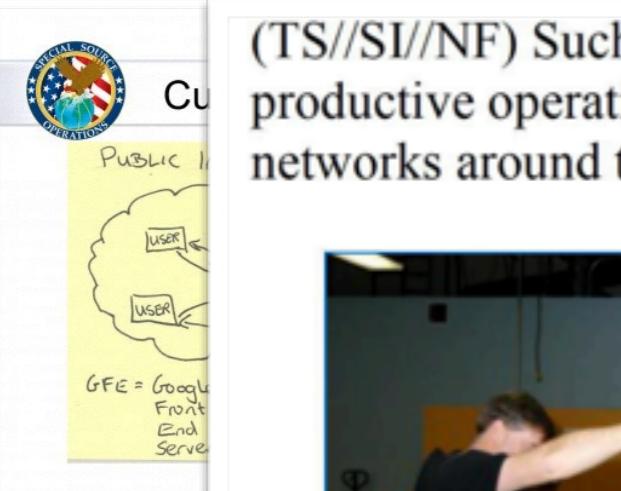
(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom

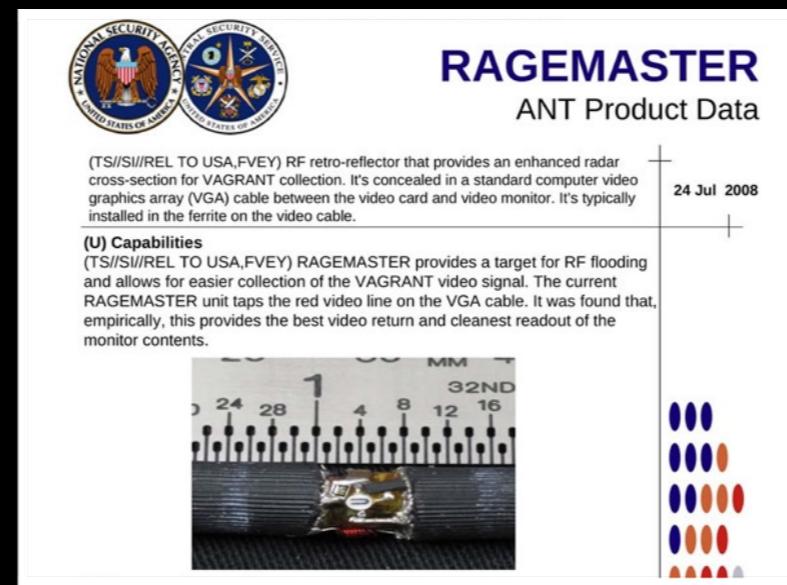
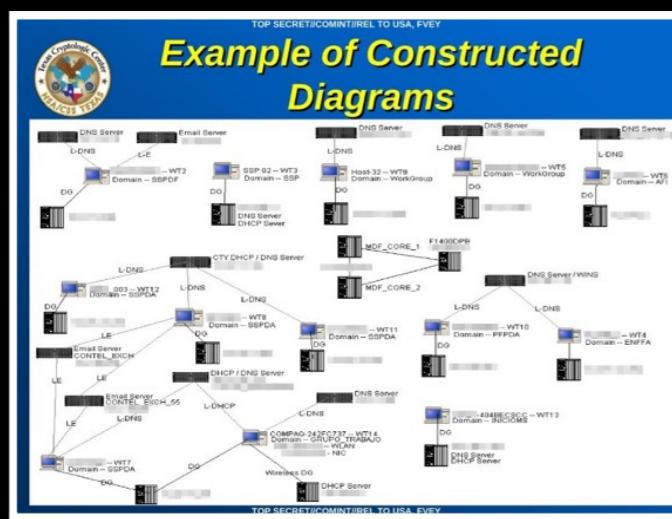
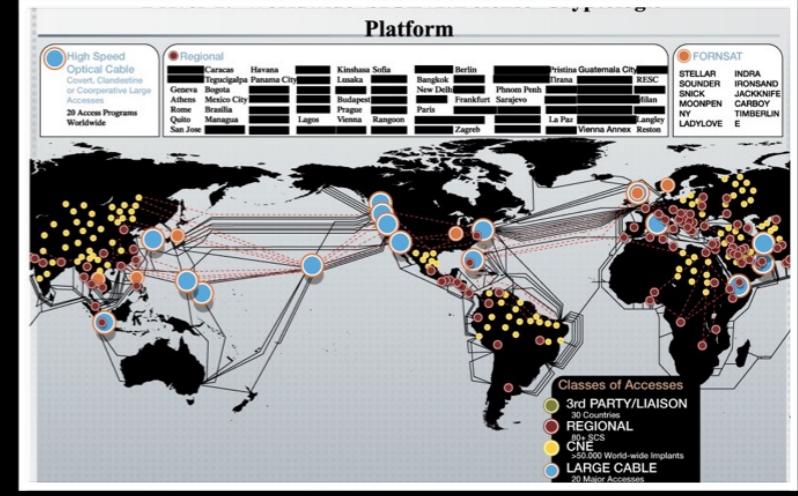
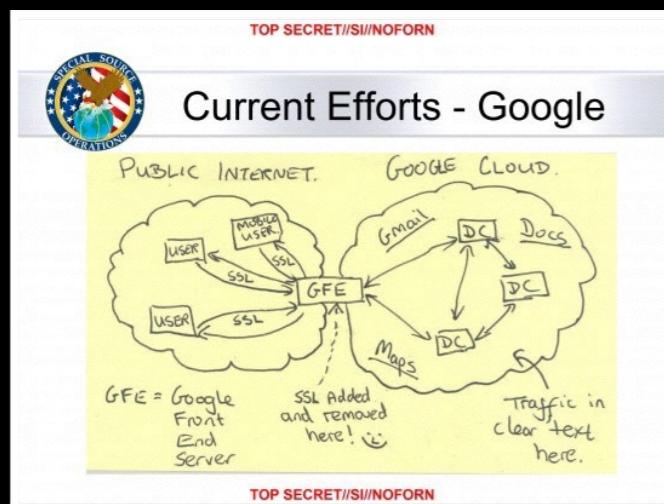
(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A “load station” implants a beacon

Was wird überwacht?

- Grundsätzlich nutzen Geheimdienste alle vorher genannten Zugangspunkte zum Datenstrom



(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.



(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

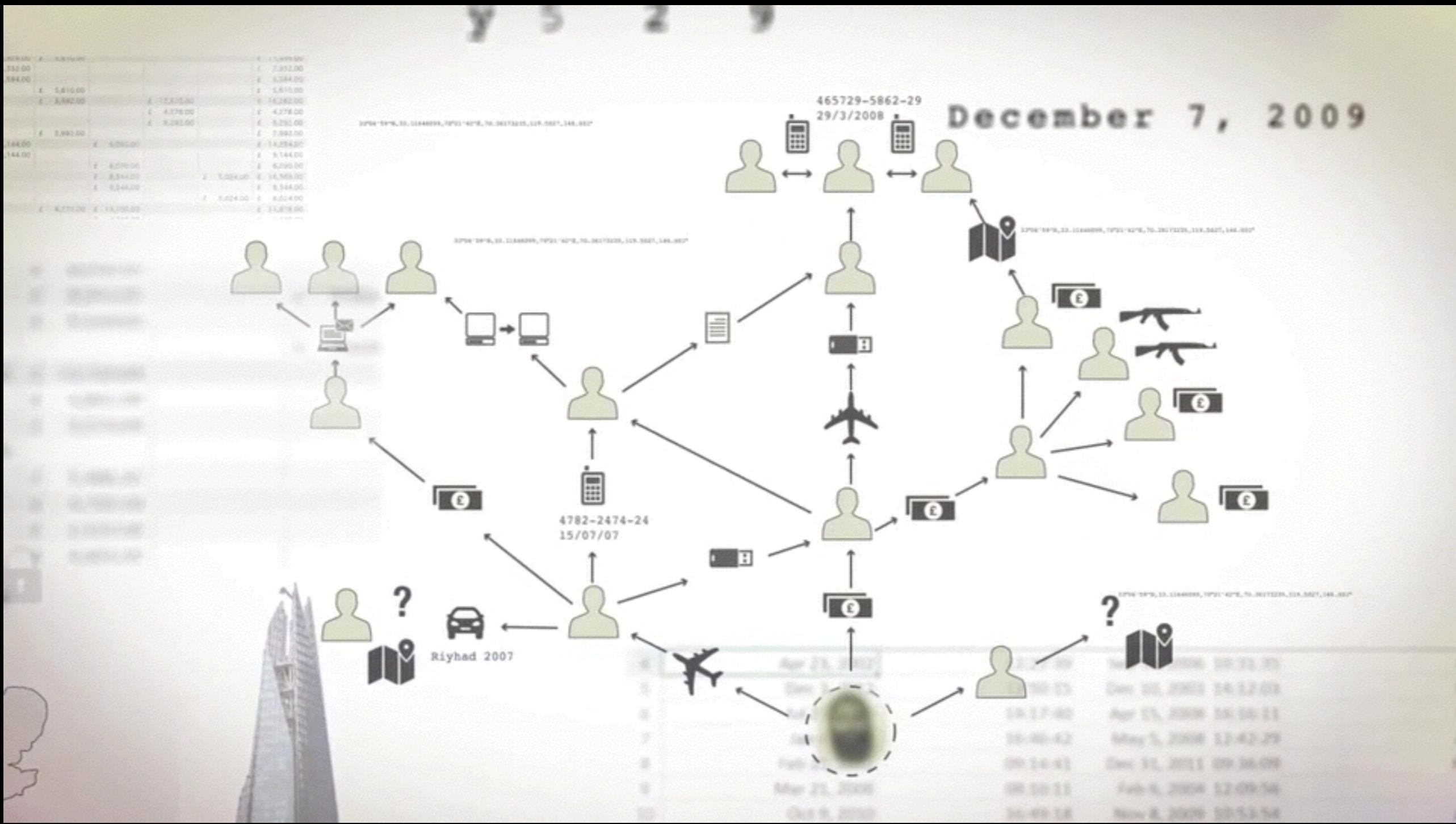
Daten

- Email
- Nachrichten (Messenger, SMS, etc.)
- Telefongespräche
- Suchanfragen
- ...

Metadaten

- Wer kommuniziert?
- Mit wem wird kommuniziert?
- Wann wird kommuniziert?
- Wie oft wir kommuniziert?
- Welche Kanäle werden genutzt?

Was kann man damit tun?



XKeyscore

- Suchmaschine für gesammelte Daten (“full-take data”)
- Aufbereitung (z.B. für Facebook Chats)
- (Fast) Echtzeitbetrachtung
- Fasst alle Erfassungspunkte zusammen
- Anomalieerkennung
- Auswahl von Zielen mittels sog. Selektieren



```
appid('social/facebook/chat/to_server', 1.0) =
    http_host('facebook.com') and
    $http_post and
    url('/ajax/chat/send.php')
: c++
extractors = {{
    login_email = /login_x=.*([a-z0-9_\-\.]{30})\$40[a-z0-9_\-\.]{30})/;
    text = /msg_text=(^&\n\r]+)/;
}}
main = {{
    if (login_email) {
        xks::user_activity_t ua("chat", "facebook");
        ua.client.add(xks::urldecode(login_email[0]), "facebook");
        ua.apply();
    }
    if (text) {
        xks::chat_body(xks::urldecode(text[0]));
    }

    return true;
}};
```

```
fingerprint('demo/scenario4') =  
    fingerprint('encryption/mojahdeen2' and  
    fingerprint('browser/cellphone/iphone')
```

- \$acwitems = 'machine gun' or 'grenade' or 'AK 47'
- \$acwpositions = 'minister of defence' or 'defense minister'
- \$acwcountries = 'somalia' or 'liberia' or 'sudan'
- \$acwbrokers = 'south africa' or 'serbia' or 'bulgaria'
- \$acwports = 'rangoon' or 'albasra' or 'dar es salam'

```
topic('wmd/acw/govtorgs') =  
    email_body($acwitems and $acwpositions and  
    ($acwcountries or $acwbrokers or $acwports));
```

NSA-UA

- Erster parlamentarischer Untersuchungsausschuss des 18. Bundestags
- Eingesetzt von allen Fraktionen am 20. März 2014
- Ausmaß und Hintergründe der Ausspähungen durch ausländische Geheimdienste aufklären
- Geladen als Zeuge sei 8. Mai 2014: Edward Snowden
- Gewährt interessante Einblicke in die Praxis des BND

Bad Aibling

- Bis 2004 Abhörstation der USA (seit 1971 NSA)
- Überlassen an den BND mit der Auflage gesammelte Daten weiterzuleiten
- Interessanterweise direkt vom BND verhandelt, nicht durch die Bundesregierung
- Zentrale Stelle für Abgreifen von Satellitenkommunikation aber auch Internet-Verkehr über direkte Leitung aus Frankfurt (DE-CIX, Operation Eikonal)



Bad Aibling liegt nicht in Bayern

Bad Aibling liegt nicht in Deutschland

Bad Aibling liegt im Weltall



Quelle: Süddeutsche Zeitung, "Die Weltraumtheorie des BND", 26. November 2014

Wie können Sie sich
dagegen schützen?

Und gegen alle anderen, die Ihre Daten wollen.

Was können Sie tun?

Verschlüsselung

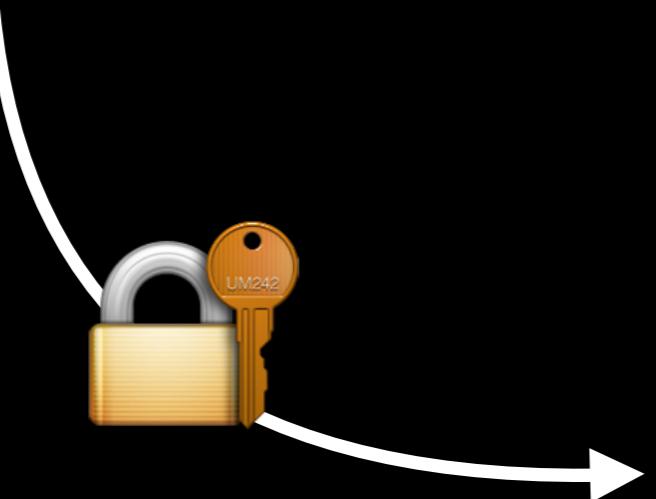
Anonymisierung

Moment mal... Hilft das nicht Kriminellen oder Terroristen?

- Stimmen nach “Hintertüren” für offizielle Stellen
- Ja, tut es aber sie finden selbst Wege das zu erreichen
- Genauso gibt es legitime Geheimhaltungswünsche (z.B. Journalisten, Whistleblower, politisch verfolgte Menschen)
- Hintertüren werden nicht nur von offiziellen Stellen genutzt werden (Was geht wird gemacht!) - Siehe AthensAffair (griechisches Telefonnetz) oder Google Backdoor Database
- Nachgewiesene Fälle von Diebstahl geistigen Eigentums (Wirtschaftsspionage)

Verschlüsselung

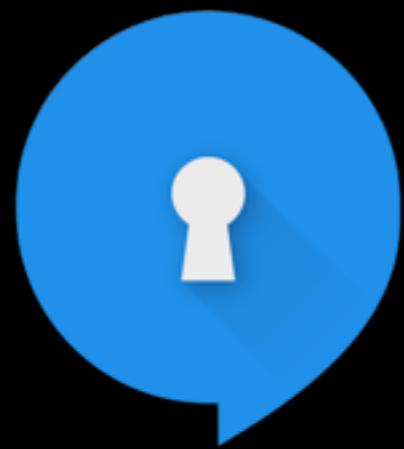
Vielen Dank, mir
geht es gut. Wir
treffen uns morgen
um 15:00 Uhr.



```
hQIMA4FXGiTYac9MARAAvMIeFXSv9MVVJ4sjdJCWqnVSL8AgQIBQ
Fi+2B6iAwymvcPDL3cLTaPSaBoEA8HHuc0HnKnZTtwFbF9lh/
iDX59UFyqQonZA9nwZ8VbzWyMu/JI
+tDs00qxByu9u3txA167NE9Q5IkjLS/
p8fIHWTEN9tx0tthGM4nQ2j9dvi0DzFrg7XQhG
+DXr0nJ9rFFXqDJQkMui5ojV4i07v3f4Jg5jEk51Ak5xhTMxk32Z
ctruruYYyqU5Bd7SAdIUfTzxD/ERYFWohk3GhPM95SxcWxy
+4o2prYe0lzV9TKStupnEGwCQnc/257FMd/
gc7wyztAC0wcJwSwKAXil/a4Ni5ZDxNY4gFicqu5I5ZEE00UB/
ReIIQeUeQ10w+nQ51KuLtt6NQkvD50v
+27DVT1iGrmzJq9WmyqgH8Gh3N7bPMMB2FwZSkdbfEDhT6mHzJzv
Yunj/kNpONyL/vCjuTVAcP
+isZkF8Dhk73gVSyp6pyTyw9j2bSCwb04AvFh+B3VtWgutr/
GkNgnZinfGfz/YnytBwpjh9HAWF5+Vx+RJ9I7JWLevHprs1C/
SfF8DY1P0TcCPCILIw4kfWVYuSM1guXhCAiPG/MF07Ui/
gRAqX47snRL2fqpDa0QRUcnQV9MQ
+D91IUJmLYT2HvuBQLbAoZTAIOYyuRY9sGSnEo7BrI9LRjShQHYI
mp2AjZdS6ERBQ0V3muBYg0yj7LxZMoB52KjGLM2Y6DW6G8Vxsswi
Sfxf1QtFMWi
+tp39L0tIDYjymXjWUGI0a8NVS0Q7sAanDhjN9vD3c3fdSOzJLEc
ixLPYd7FwjY1MRCJo0kHAi0Dc5fP9na2DfiL2tIZs3t4twLkKRQ
AH7FjcU=
```

Wie kann ich das nutzen?

- Kommunikation -



Signal

SMS
Anrufe



Telegram

Messenger



Threema

Messenger

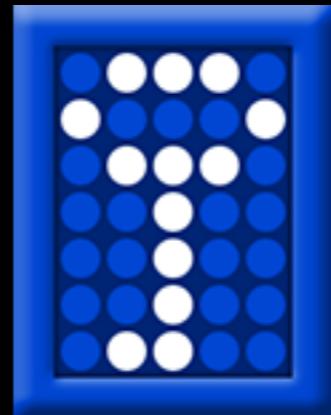


GnuPG

E-Mail
Dateien

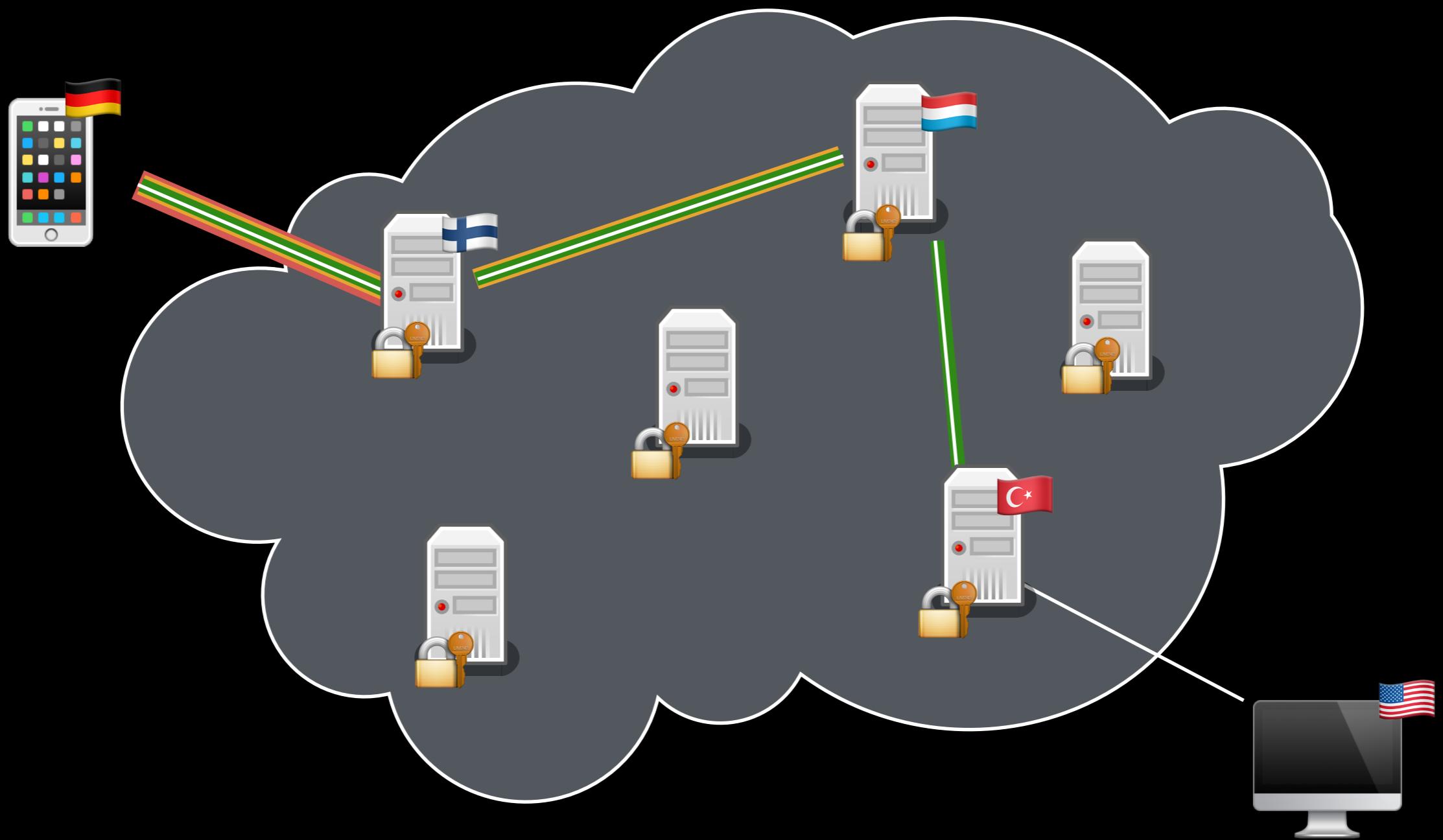
Wie kann ich das nutzen?

- Datenträger -



TrueCrypt

Anonymisierung



Wie kann ich das nutzen?



Tor Browser

Anonymer Browser
Windows / Mac / Linux



Orbot

Android App
Kann den kompletten
Datenverkehr über Tor
abwickeln



Tails

Linux Live System
Anonymes,
"vergessliches", Linux
System von CD, DVD
oder USB-Stick

Zusammenfassung



Welche Spuren hinterlassen
wir im Internet?



Was kann man damit tun?



Wie kann ich das nutzen?



Vielen Dank

Ben Hermann

 @benhermann

Quellen

- Ausschnitt aus Glenn Greenwalds Artikel für den Guardian (06. Juni 2013)
<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>
- Ausschnitt aus Laura Poitras Videomaterial für den Guardian (11. Juni 2013)
<http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>
- Photos MfS Disguise Seminar (Archived by Simon Menner)
<http://simonmenner.com/pages/Stasi-DisguiseSeminar.htm>
- Video Egelsbach Transmitter Station (September 2014, freundlicherweise überlassen von Andreas J. Pilot)
- Audio E05 Cynthia (Aufnahme von Simon Mason)
<http://www.simonmason.karoo.net/page65.html>
- Bundeshaushalt 2015
<http://www.bundeshaushalt-info.de/#/2015/soll/ausgaben/einzelplan/0404.html>
- US Black Budget
<http://www.washingtonpost.com/wp-srv/special/national/black-budget/>
- Bildquelle Überwachungsanlage Bad Aibling: REUTERS
- Weltraumtheorie des BND
<http://www.sueddeutsche.de/politik/nsa-ausschuss-des-bundestags-das-zweifelhafte-gebaren-von-bnd-und-bundesregierung-1.2238644-3>
- MI6 Werbevideo
<https://www.sis.gov.uk/io-video-profile-amelia.html>
- SIA funding website
<https://www.mi5.gov.uk/home/about-us/who-we-are/funding.html>

Quellen

- Athens Affair
<http://spectrum.ieee.org/telecom/security/the-athens-affair>
- Google Backdoor Database
https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html
- XKeyscore und Selektoren
https://www.schneier.com/blog/archives/2015/07/more_about_the_.html
<https://theintercept.com/document/2015/07/01/xks-counter-cne/>
<https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/>
<https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/>
- Anzeige wegen §99 StGB
<http://www.spiegel.de/politik/deutschland/bnd-spion-markus-r-wegen-landesverrats-angeklagt-a-1049010.html>

Softwarelinks

- Signal
<https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en>
<https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8>
- Telegram
<https://play.google.com/store/apps/details?id=org.telegram.messenger&hl=en>
<https://itunes.apple.com/en/app/telegram-messenger/id686449807?mt=8>
- Threema
<https://play.google.com/store/apps/details?id=ch.threema.app&hl=en>
<https://itunes.apple.com/en/app/threema/id578665578?mt=8>
- GnuPG
<https://www.gnupg.org/>
- TrueCrypt (Achtung! Keine Weiterentwicklung mehr!)
<http://truecrypt.sourceforge.net/>
- Tor Browser
<https://www.torproject.org/projects/torbrowser.html.en>
- Orbot
<https://play.google.com/store/apps/details?id=org.torproject.android&hl=en>
- Tails
<https://tails.boum.org/>