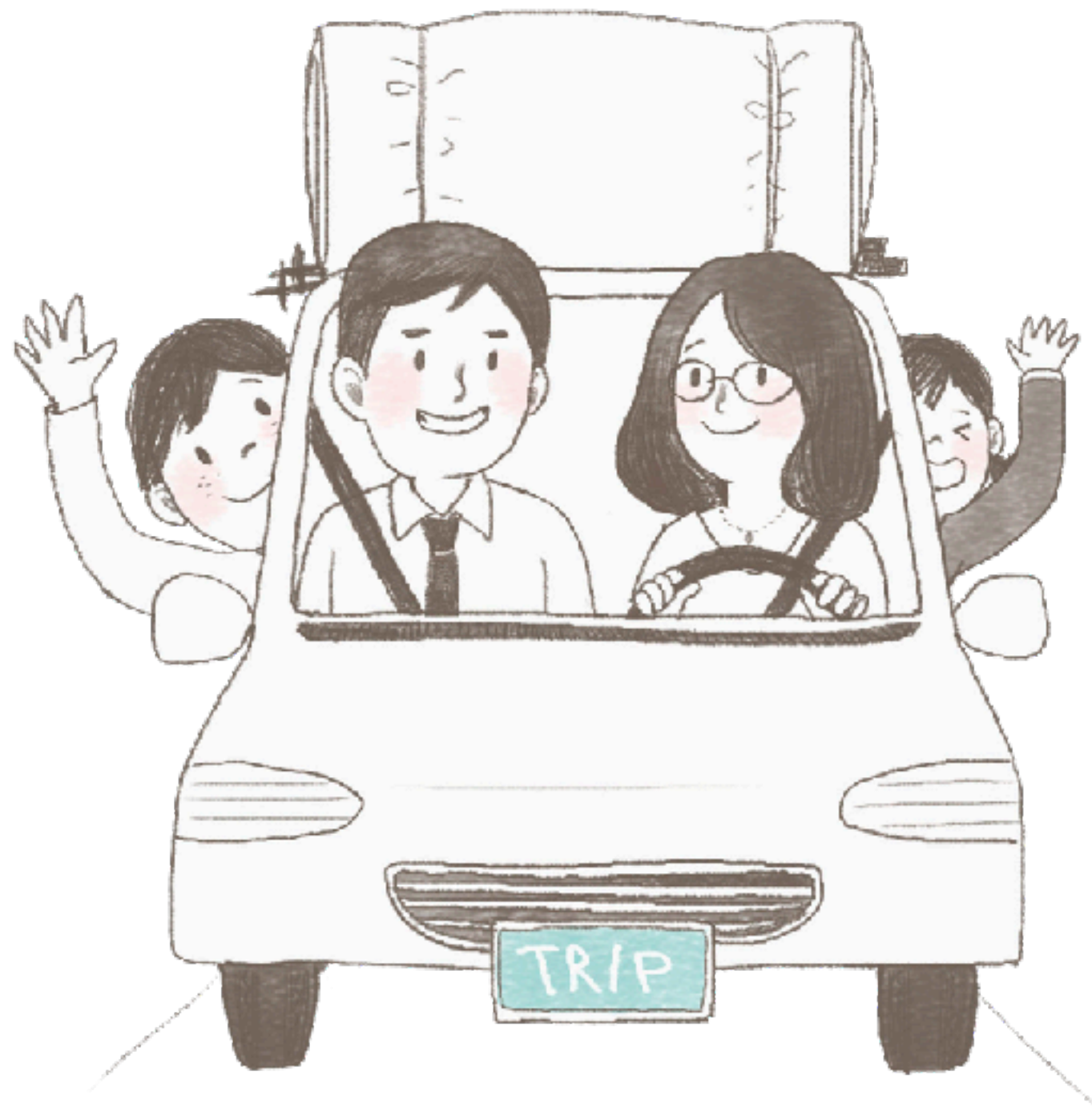
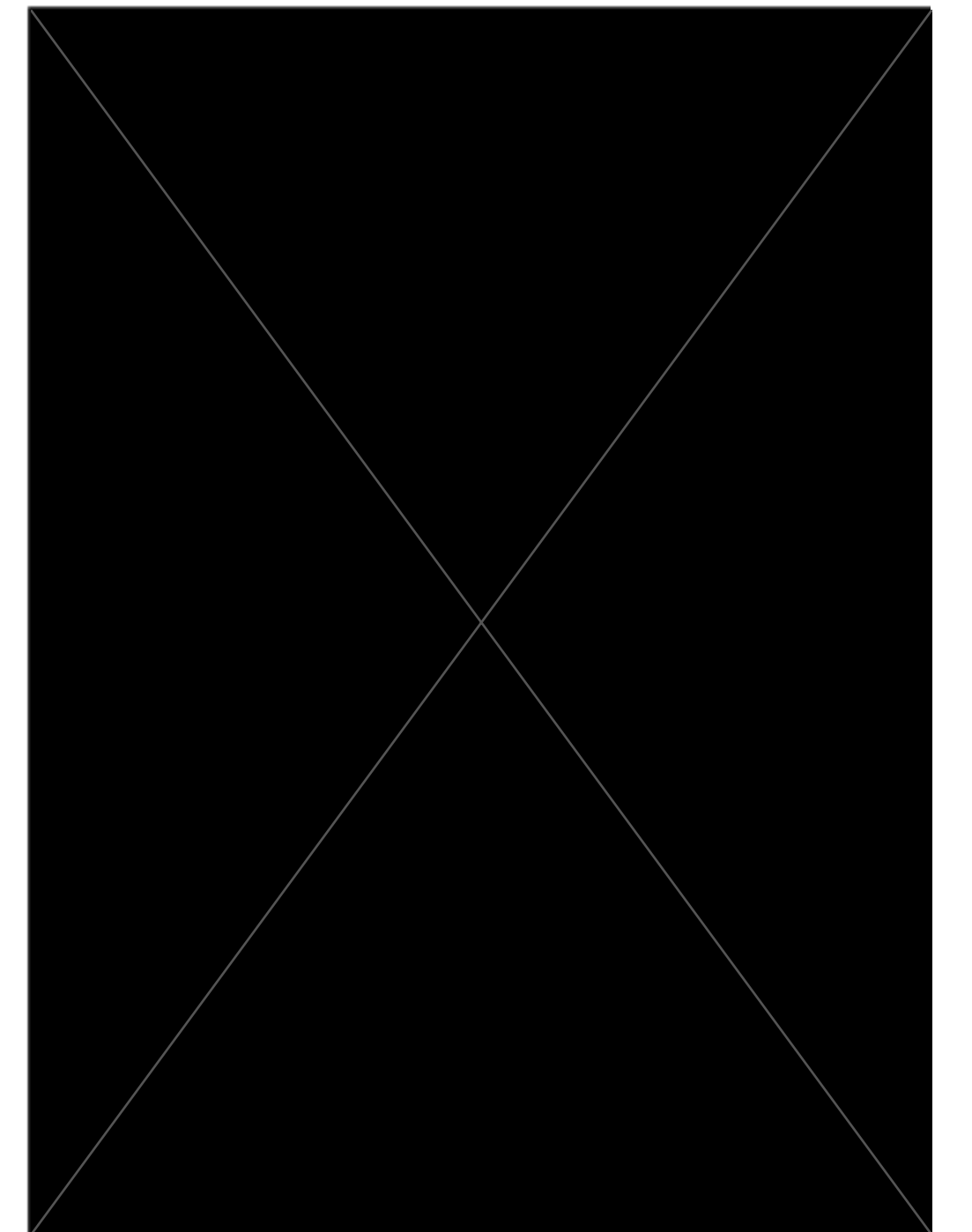


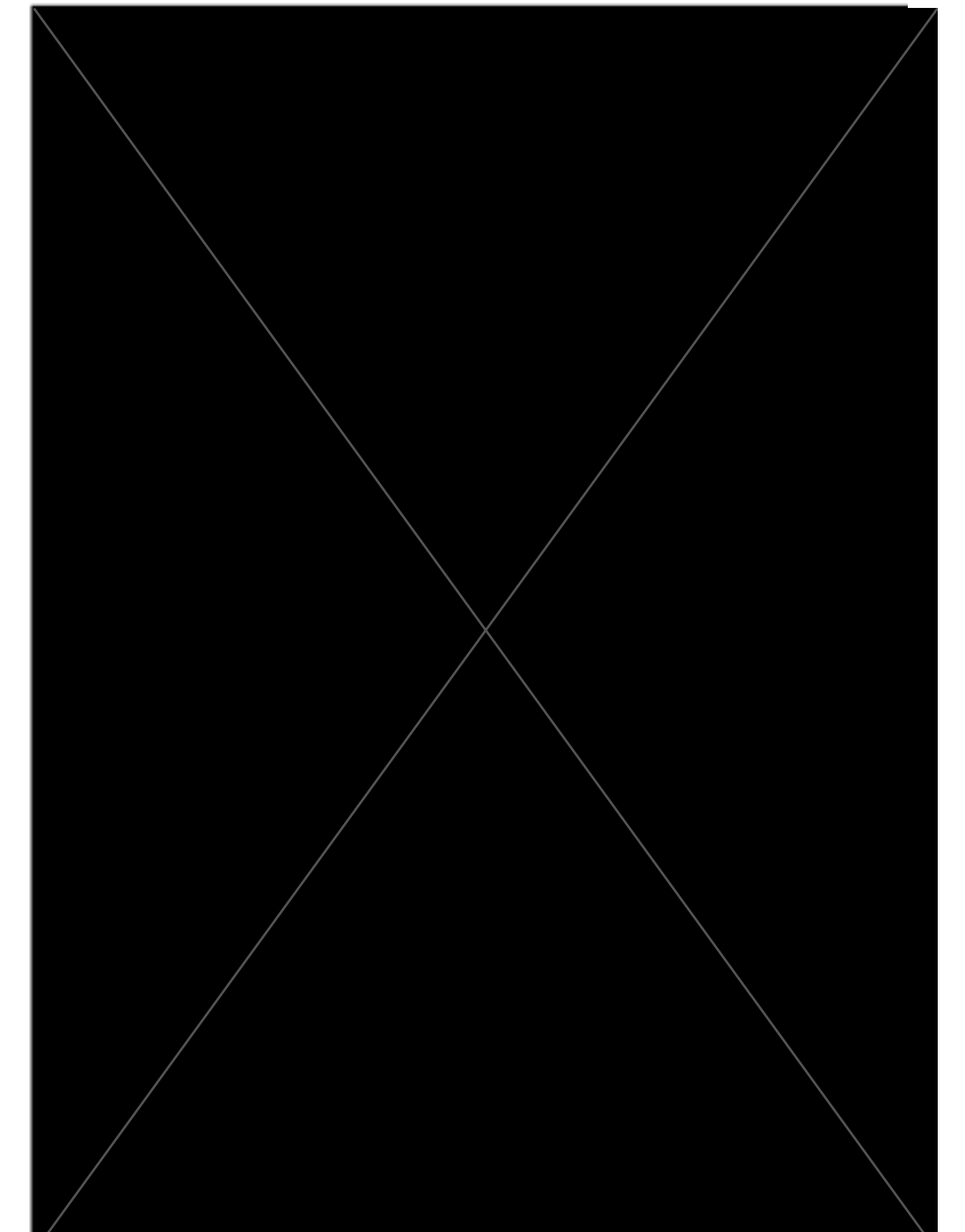


Ausflug in's Dark Web

Bevor's los geht ..

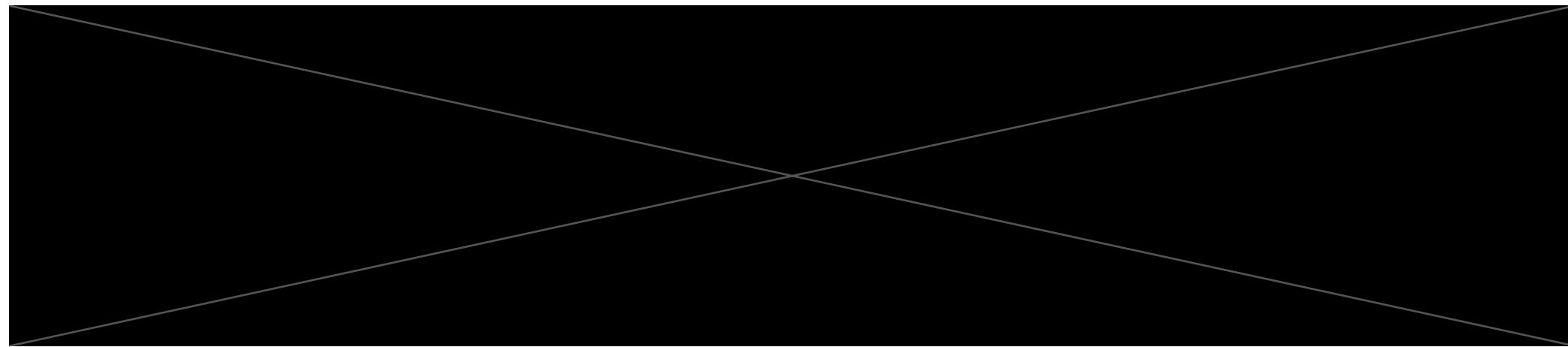


Bevor's los geht ..

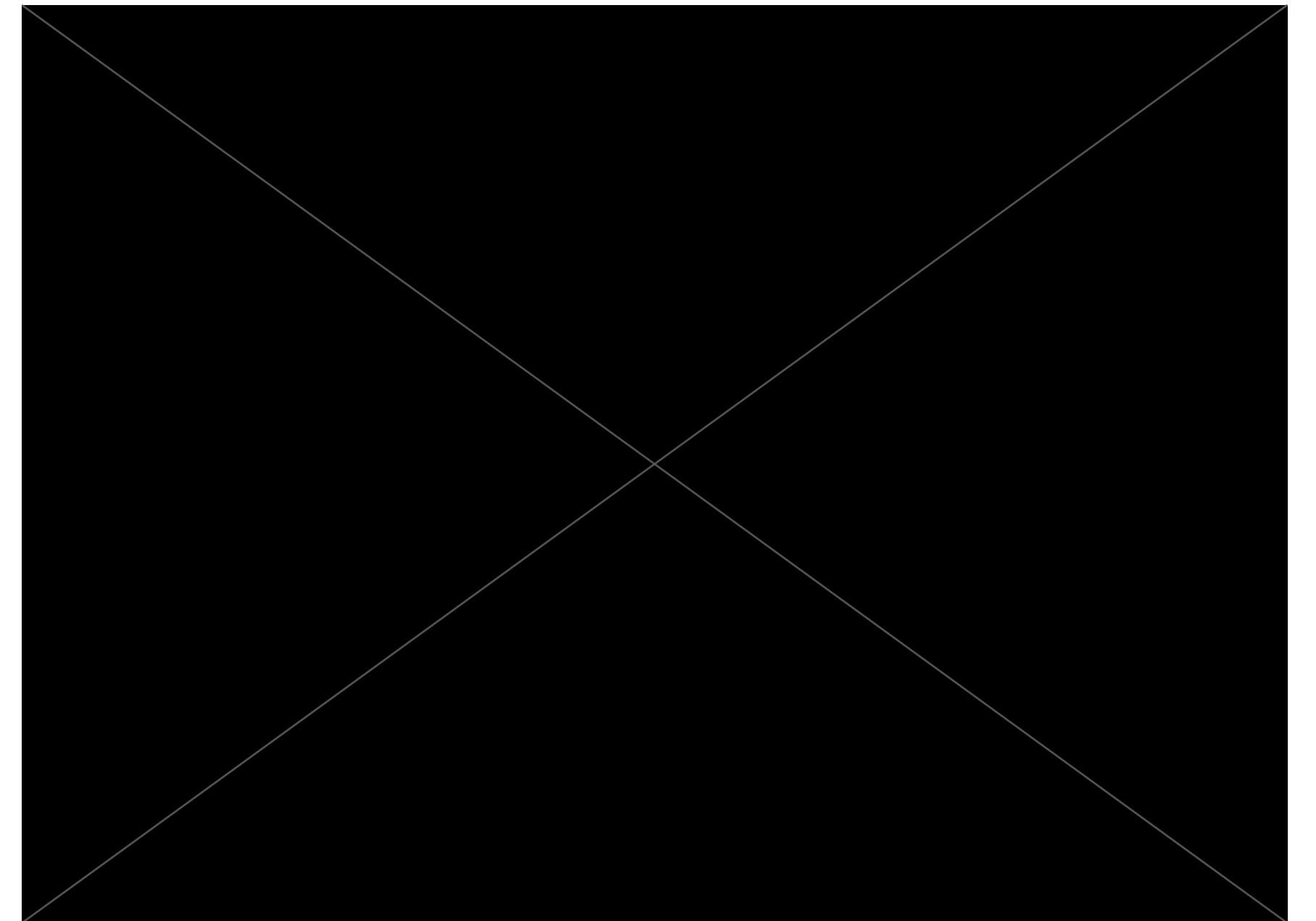


Der, die, das, wer, wie, was?

Vor allem: wer?

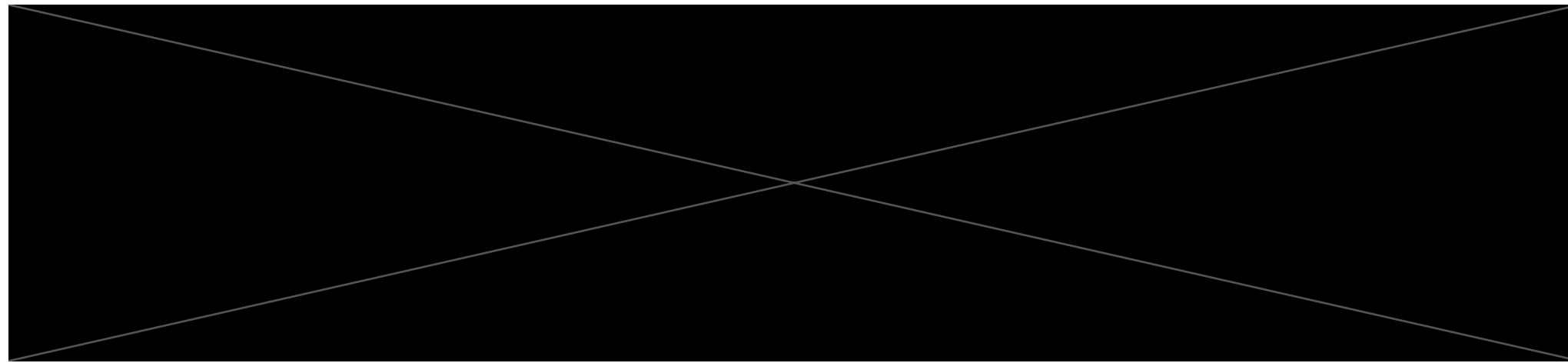


- Fokus auf strategische Threat Intelligence
 - Langfristige Bedrohungsanalyse

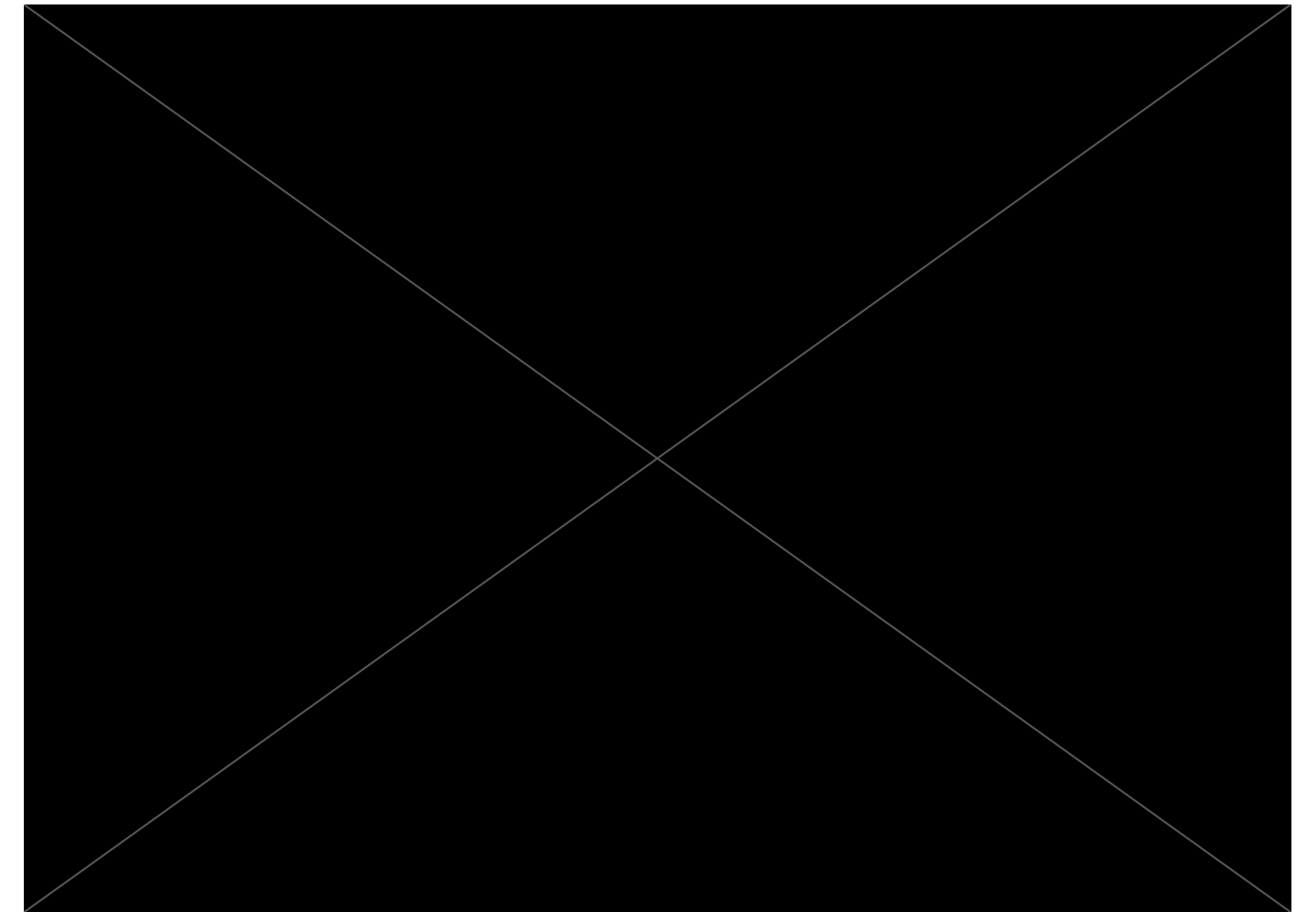


Der, die, das, wer, wie, was?

Vor allem: wer?

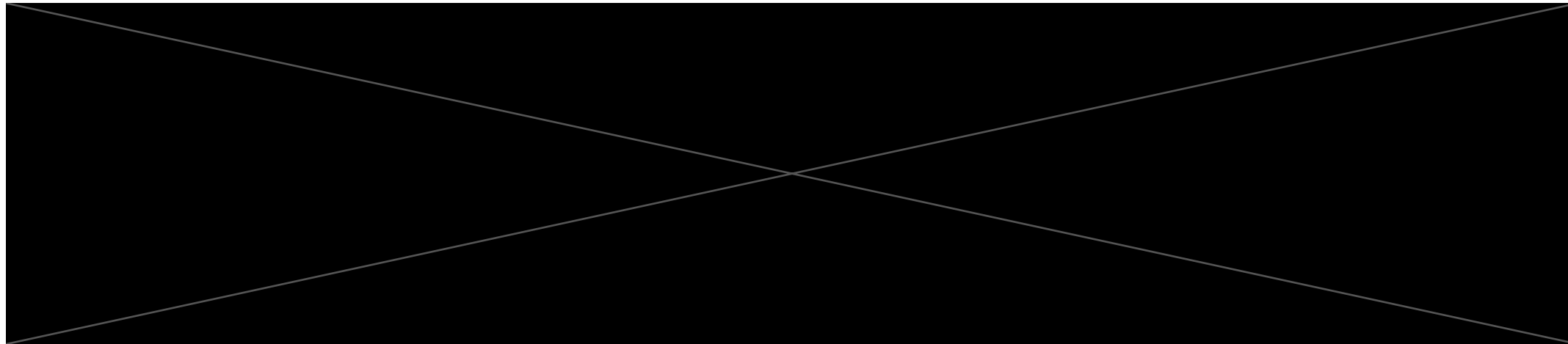


- Fokus auf strategische Threat Intelligence
 - Langfristige Bedrohungsanalyse



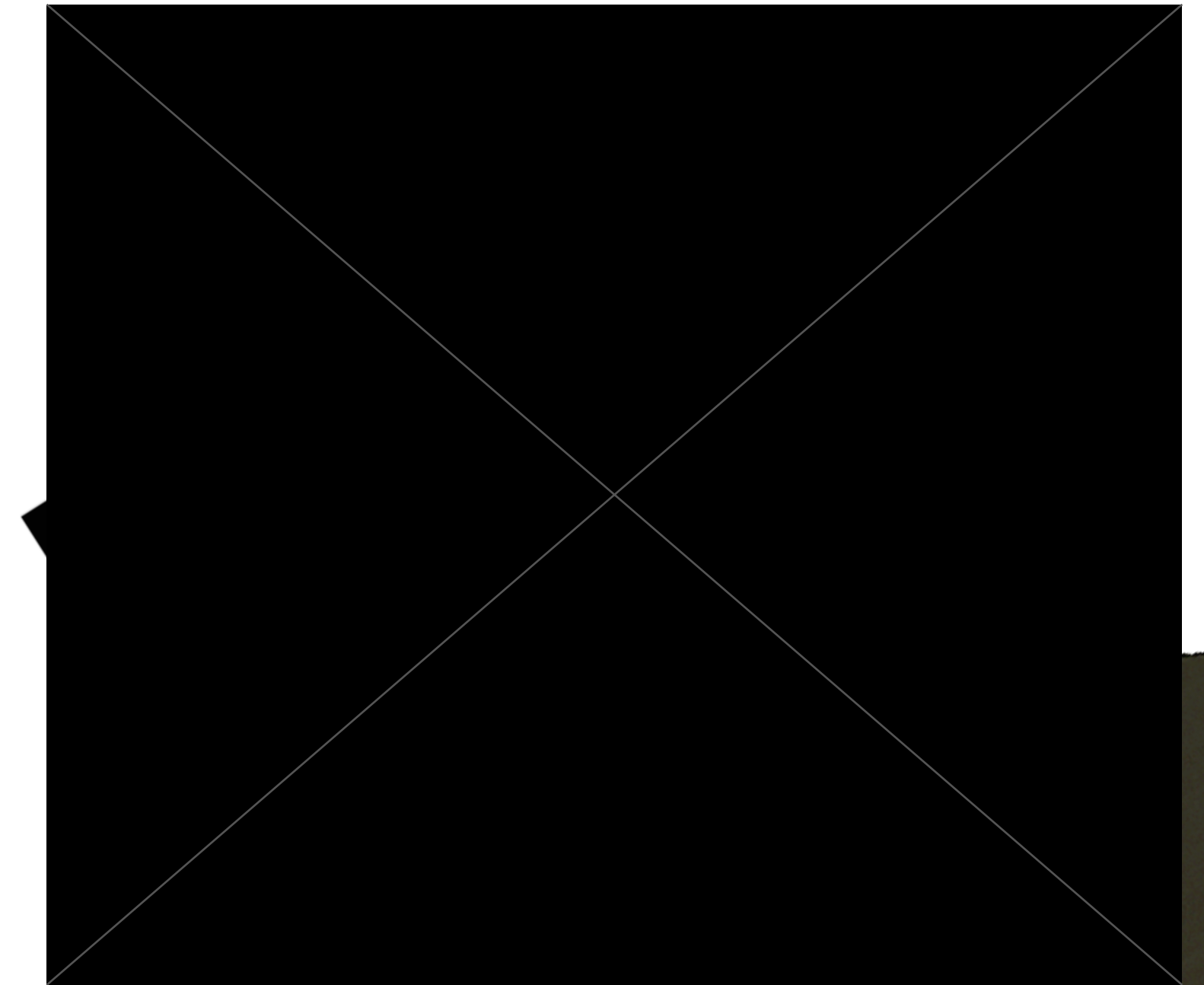
Der, die, das, wer, wie, was?

Vor allem: wer?



- Fokus auf strategische Threat Intelligence
 - Langfristige Bedrohungsanalyse

BITTE KEINE FOTOS / SOCIAL MEDIA



Dark Web?



“Dark Web” bezeichnet einen Teil des Internets, der nicht ohne den Einsatz spezieller Software zugänglich ist.

(c) ich, ungefähr zwei Stunden vor Vortragsbeginn

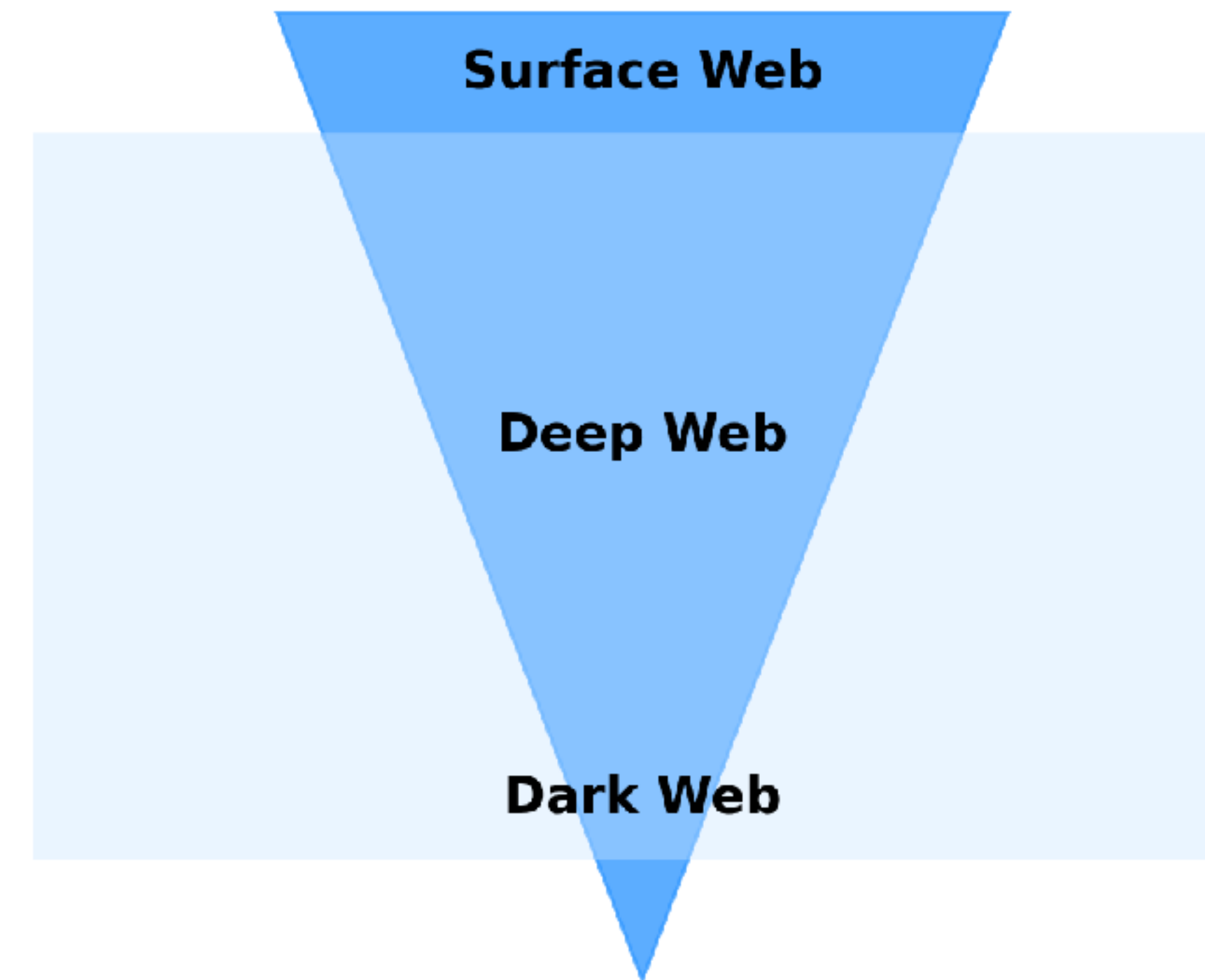
Das Internet als Eisberg

- **“Surface Web”**
 - Von Suchmaschinen indizierte Inhalte
- **“Deep Web”**
 - Datenbanken, Cloudspeicher, ..
- **“Dark Web”**
 - Benötigt spezielle Software



Das Internet als Eisberg

- **“Surface Web”**
 - Von Suchmaschinen indizierte Inhalte
- **“Deep Web”**
 - Datenbanken, Cloudspeicher, ..
- **“Dark Web”**
 - Benötigt spezielle Software



Tor Project

“The Onion Router”

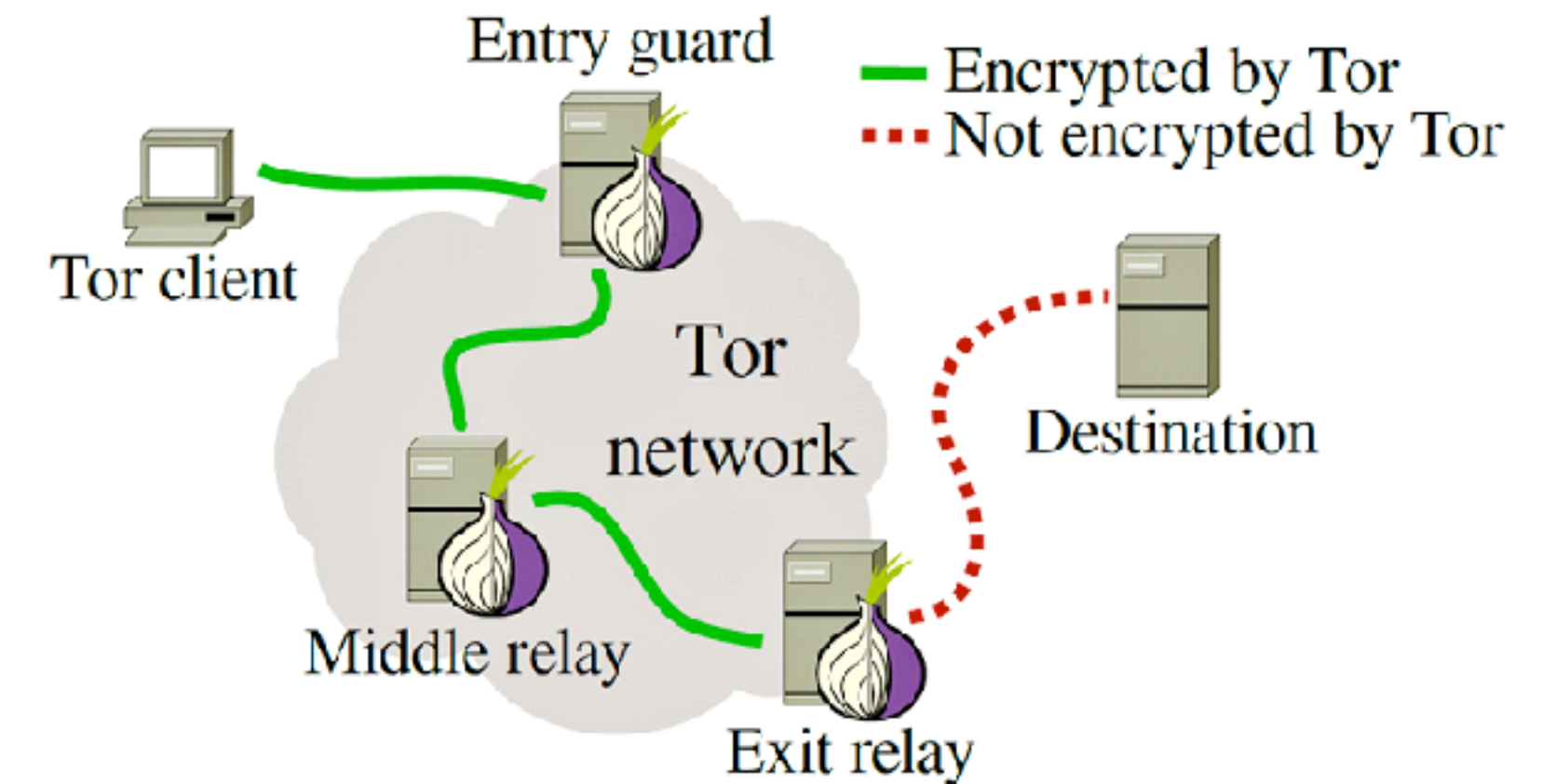
- **2002 gegründet**
 - Seit 2006 durch Non-Profit verwaltet
- **Sponsoren aus allen Ecken und Enden**
 - Inklusive Regierungen und Militärs
- **Entwickelt und “betreibt” das “Tor-Netzwerk”**



Tor-Netzwerk? Zwiebelschalen!

Wie das Tor-Netzwerk funktioniert

- **Leitet Verbindungen durch mehrere “Knoten”**
 - Eintrittsknoten (“Entry Node”)
 - Mittelknoten (“Middle Nodes”)
 - Ausgangsknoten (“Exit Node”)
- **Verbindungen erfolgen verschlüsselt**



Tor-Netzwerk? Zwiebelschalen!

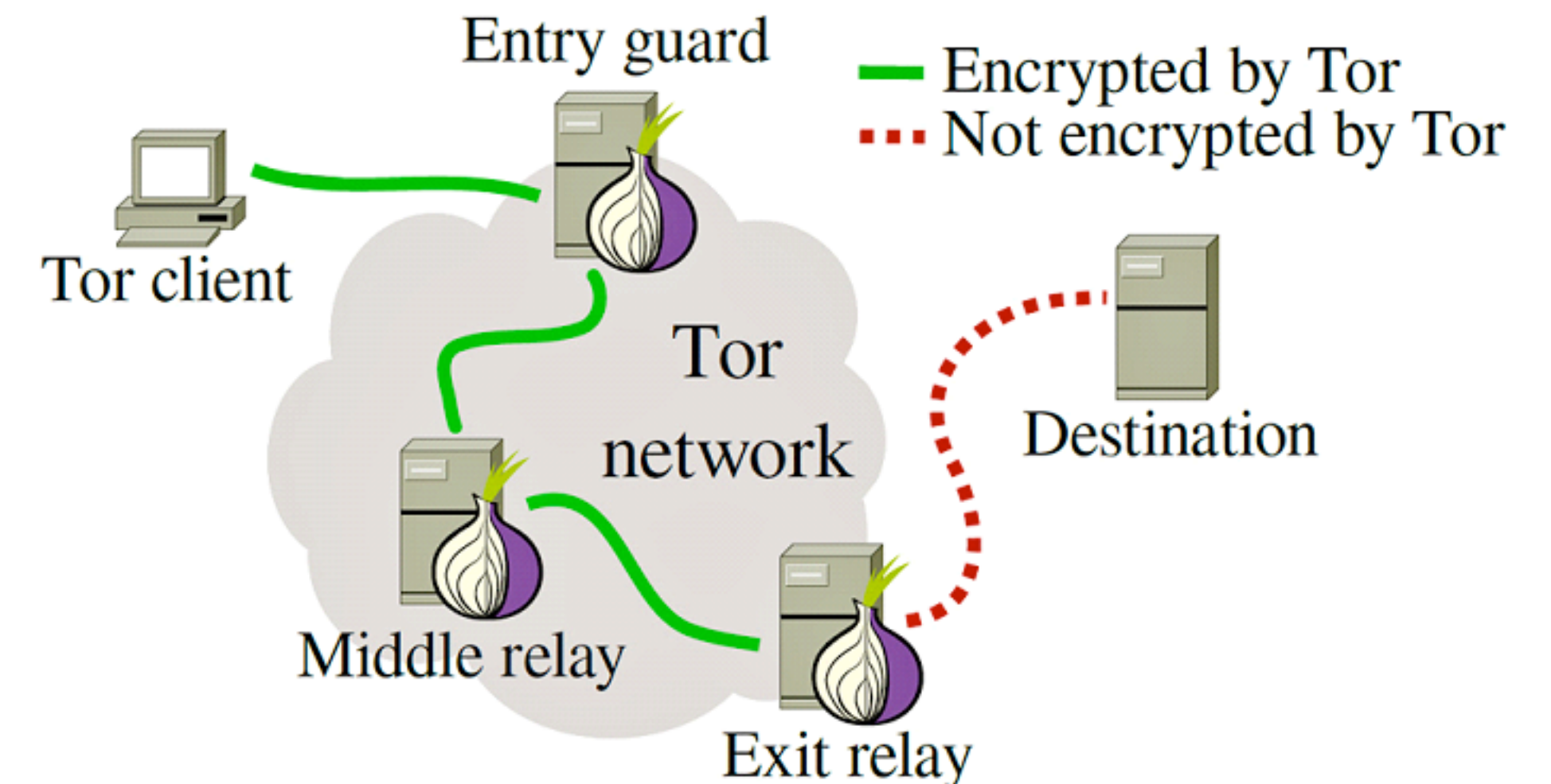
Das hat Vorteile. Und Nachteile.

- **Vorteile**

- Kein Knoten kennt gesamten Pfad
- Dynamische Routen

- **Nachteile**

- Exit-Nodes können “mitlesen”
- Manipulation des Netzwerkes durch bösartige Knoten
- Nachteile als Nutzer:in (Geschwindigkeit, Sperren)



Zwiebel schneiden nutzen

Tor Browser

- **Beliebtestes / einfachstes Werkzeug**
 - Mozilla Firefox 🤝 Tor-Client vorkonfiguriert
 - Alle Verbindungen über das Tor-Netzwerk
- **Erlaubt auch Zugriff auf Webseiten im Tor-Netzwerk**



.. Webseiten *im* Tor-Netzwerk?

Eine neue Welt öffnet sich!

Eine neue Welt öffnet sich!



“Onion Service”

- Webseiten oder Dienste die nur über Tor erreichbar sind
 - Traffic verlässt das Tor-Netzwerk nicht
 - Vollständige Verschlüsselung des Verkehrs
- Nutzen eigene Domain, “.onion”



“Onion Service”

- **Anonymität für Betreiber:innen und Nutzer:innen**
 - Betreiber:in sieht nur IP-Adressen von Tor-Nodes
 - IP-Adresse des Servers (meist) versteckt
- **Zensurresistenz**
 - DNS-Sperren oder IP-Blockaden sind wirkungslos
 - DDoS-Angriffe erschwert

“Onion Service”

- **Vertrauensthematik**
 - Jede:r kann einen Onion Service betreiben
 - Keine Authentifizierung, außer man ist Facebook
- **Performance**
 - Limitierte Geschwindigkeit
- **Aufwand**
 - Technische Mehrarbeit

“Onion Service”

Onions are a criminals best friend. <3

- Ohne Frage viele legitime Zwecke, aber ..
- Onion Services werden **gerne** für kriminelle Zwecke eingesetzt
 - “Brot und Butter” in der Sicherheitsbranche

“Onion Service”

Onions are a criminals best friend. <3

- Ohne Frage viele legitime Zwecke, aber ..
- Onion Services werden **gerne** für kriminelle Zwecke eingesetzt
 - “Brot und Butter” in der Sicherheitsbranche



Ich hab 'ne Zwiebel auf dem Kopf ..

.. ich bin kriminell!

- **Cybercrime-as-a-Service**
 - Ransomware-as-a-Service, DDoS-as-a-Service
 - Bulletproof Hosting
- **Ökosystem “Fraud”**
 - Gefälschte Dokumente, gestohlene Finanzdaten
 - “Money Mules”



Ich hab 'ne Zwiebel auf dem Kopf ..

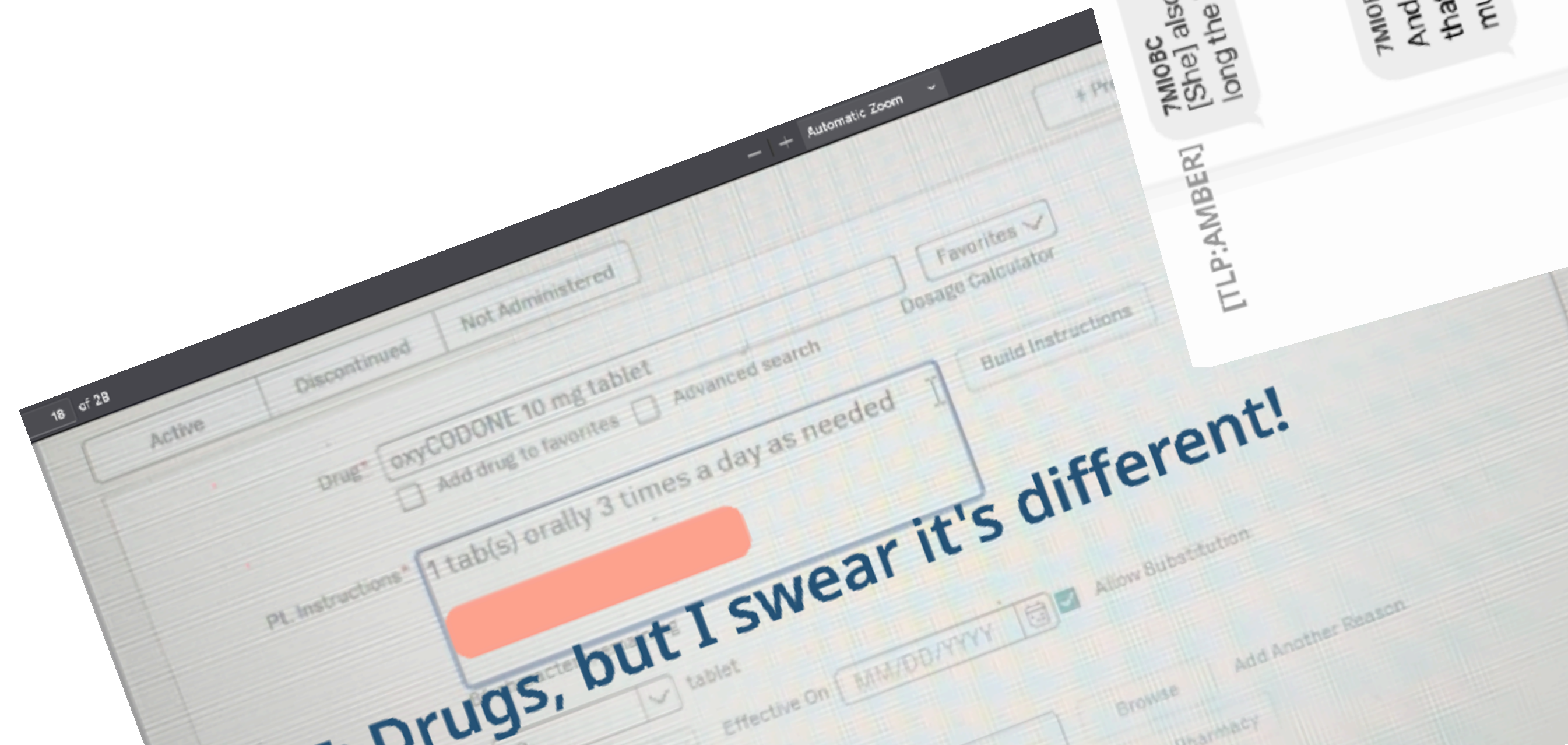
.. ich bin kriminell!

- **Digitale Marktplätze**
 - Drogen, gefälschte Dokumente
 - (Eingeschränkt) Waffen, eher “waffennahe” Güter
- **Gestohlene Daten**
 - Benutzer:innendaten, personenbezogene Daten, ..

Werbung aus Zeitgründen

(Nein, ernsthaft)

- Kriminalität in digitalen Räumen ist eigenes Thema
- Ich habe dazu geschrieben und wiederholt gesprochen
 - Bei Interesse: Ping me!



Good cop ..

Die Polizei ist immer und über-all!

- Undercover-Ermittlungen
- Analyse von Kryptowährungen
- Transnationale Kooperation



Bad cop ..

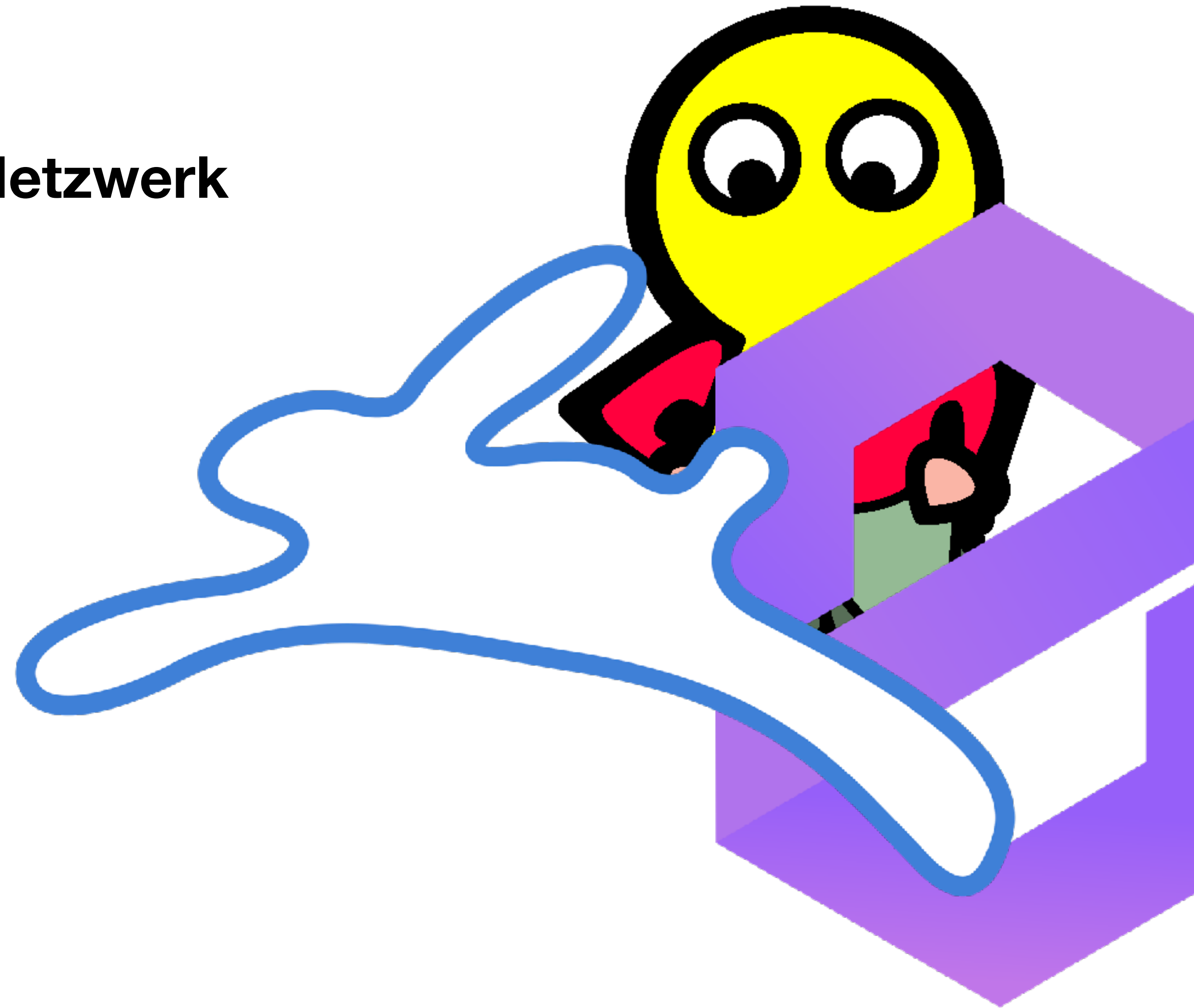
Die (böse) Polizei ist immer und über-all!

- Undercover-Ermittlungen
- Analyse von Kryptowährungen
- Transnationale Kooperation



Da ist noch mehr .. viel mehr!

- Tor ist das bekannteste Projekt / Netzwerk
- **Definitiv nicht das Einzige**
 - I2P (“Invisible Internet Project”)
 - Lokinet
 - Freenet
- Auch hier: **Bewusster Umgang!**



~~Live Demo~~ Case Studies

- **Juristisch riskant**
 - IANAL, aber CSAM am Beamer .. suboptimal
- **Verantwortungstechnisch riskant**
 - Fragwürdige Inhalte sind Realität
- **Technisch riskant**
 - Stabilität im Dark Web ist .. so eine Sache

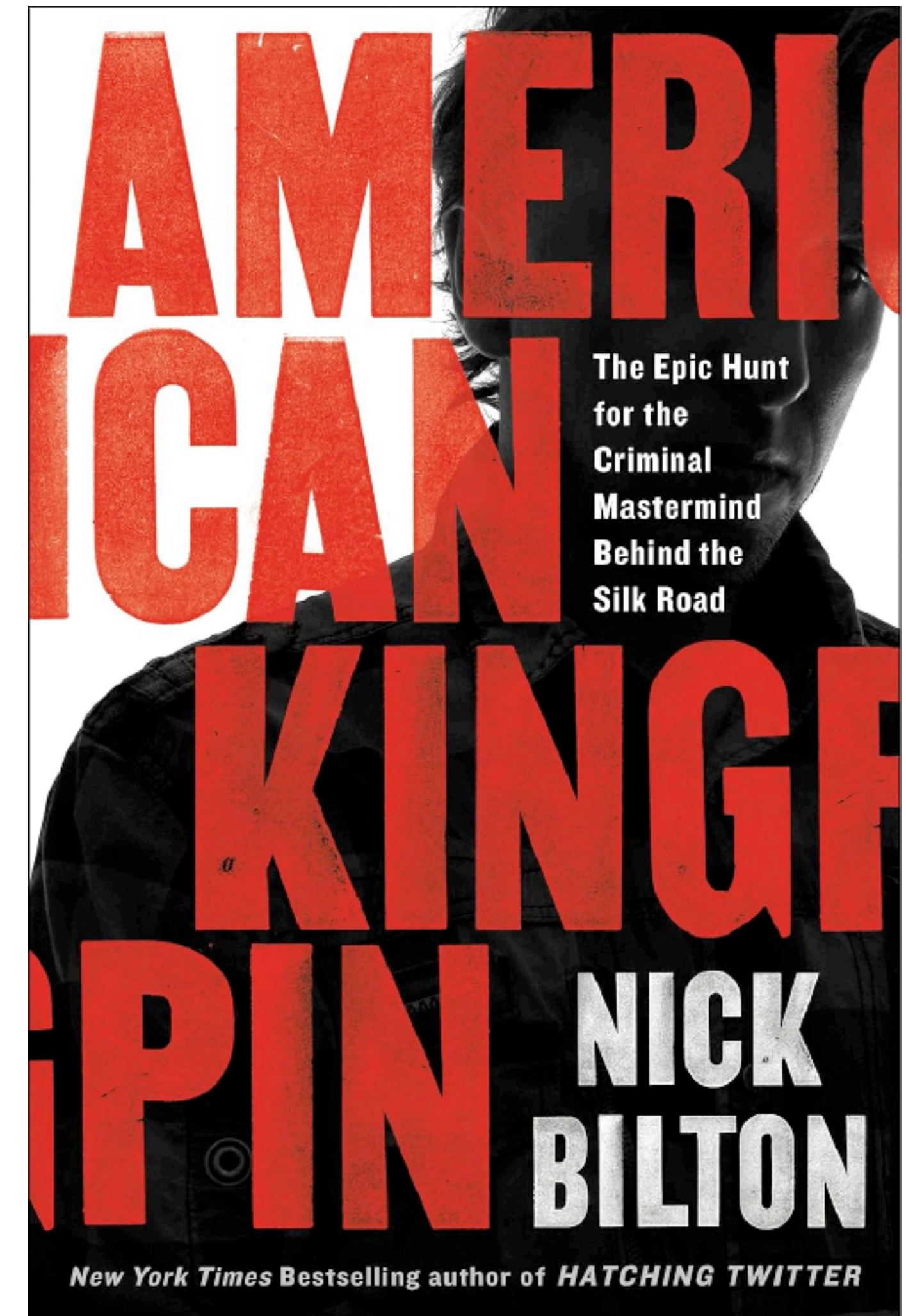
I - Silk Road

- **Erster großer “Dark Web Market”**
 - 2011 - 2013 aktiv, >1 Milliarde Dollar Umsatz
- **Gegründet durch Ross Ulbricht**
 - 2013 verhaftet, 2025 begnadigt
- **Inspiration für viele Marktplätze**
 - Gleichzeitig Beweis, dass LEA nicht machtlos ist



I - Silk Road

- **Erster großer “Dark Web Market”**
 - 2011 - 2013 aktiv, >1 Milliarde Dollar Umsatz
- **Gegründet durch Ross Ulbricht**
 - 2013 verhaftet, 2025 begnadigt
- **Inspiration für viele Marktplätze**
 - Gleichzeitig Beweis, dass LEA nicht machtlos ist



II - Daphne Caruana Galizia

Lebensschutz durch Anonymität

- Maltesische investigative Journalistin
- Nutzte (vor allem) Tor für sichere Kommunikation
 - PGP-verschlüsselte Tor-only Mails
 - Instant Messaging über Tor
- 2017 durch eine Autobombe ermordet
 - “JeTzT üBeRtRelb MaL nIcHt”



II - Daphne Caruana Galizia

Lebensschutz durch Anonymität

- Maltesische investigative Journalistin
- Nutzte (vor allem) Tor für sichere Kommunikation
 - PGP-verschlüsselte Tor-only Mails
 - Instant Messaging über Tor
- 2017 durch eine Autobombe ermordet
 - “JeTzT üBeRtRelb MaL nIcHt”



Vorwarnung

III - “Welcome to Video”

Yes, this is (sadly) a thing.

- Als Onion-Service gehostete “Tauschbörse”
 - Nutzer:innen konnten “points” kaufen / verdienen
 - 4.000 zahlende Mitglieder aus 38 Ländern
 - 45% für LEO unbekanntes Material
- Unsichere Systeme ermöglichten Ermittlungen
 - 337 Festnahmen in 38 Ländern



III - “Welcome to Video”

Yes, this is (sadly) a thing.

- **Es gibt CSAM und CSAM-Communities im Tor-Netzwerk**
 - LEA nimmt das Thema ernst und ist dahinter
- **80% der Verbreitung von CSAM passiert im “Clearnet”**
 - LEA nimmt das Thema ernst und ist dahinter
 - Plattformen .. oftmals weniger
- **Österreich ist engagiert!**
 - stopline.at



IV - Sichere Kommunikation für Gefährdete

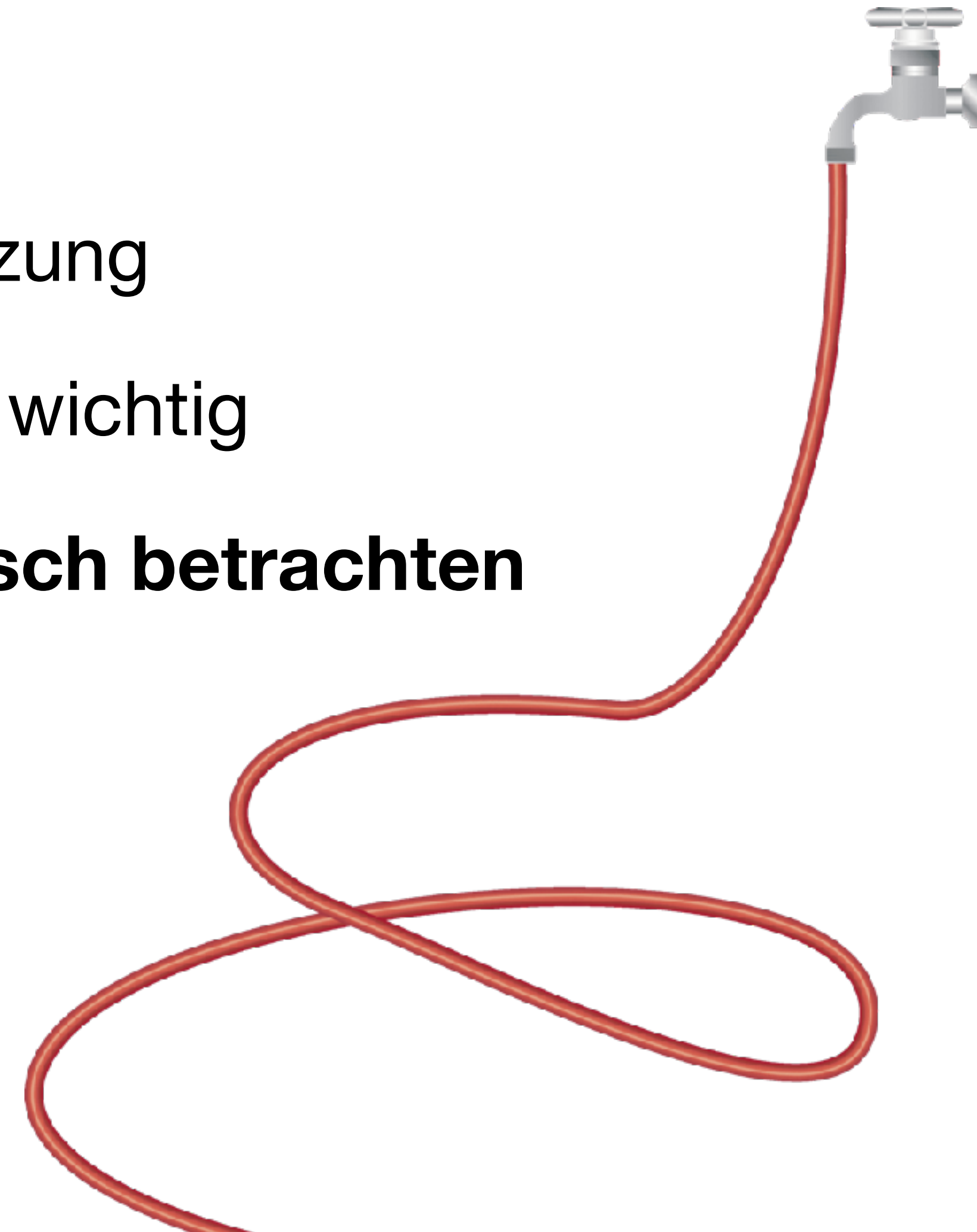
Opfer von Gewalt, queere Communities, ..

- **NGOs und Hilfsorganisationen bieten Onlineberatungen über Tor an**
 - z.B. Hilfetelefon “Gewalt gegen Frauen”
- **Gefährdete queere Communities nutzen Tor zum Schutz vor Repression**
 - z.B. “Russian LGBT Network”
- **Aktivist:innen nutzen Onion Service für den Informationsaustausch**
 - z.B. Videos von iranischer Polizeigewalt via OnionShare

Das war jetzt viel ..

TL;DR

- **(Nicht nur) ein Ort der Illegalität**
 - Viel Kriminalität, aber auch viel (wichtige) legale Nutzung
- **Wertvolles Werkzeug**; verantwortungsvoller Umgang wichtig
- **Nutzen und Risiken verstehen, Behauptungen kritisch betrachten**
 - Insbesondere in .. “Qualitätsmedien”
 - Viel Schall und Rauch!



Danke für die Aufmerksamkeit.

- Falls es noch Fragen gibt - jetzt ist der beste Zeitpunkt!

