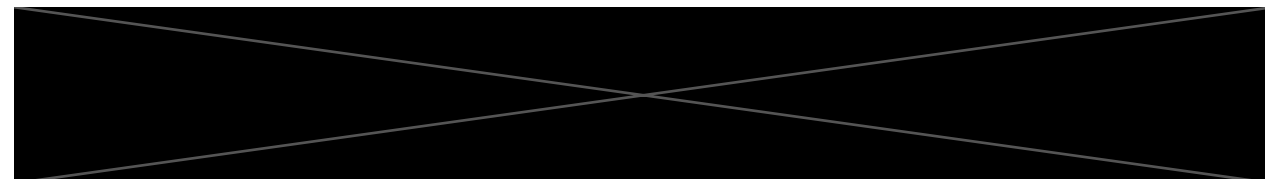


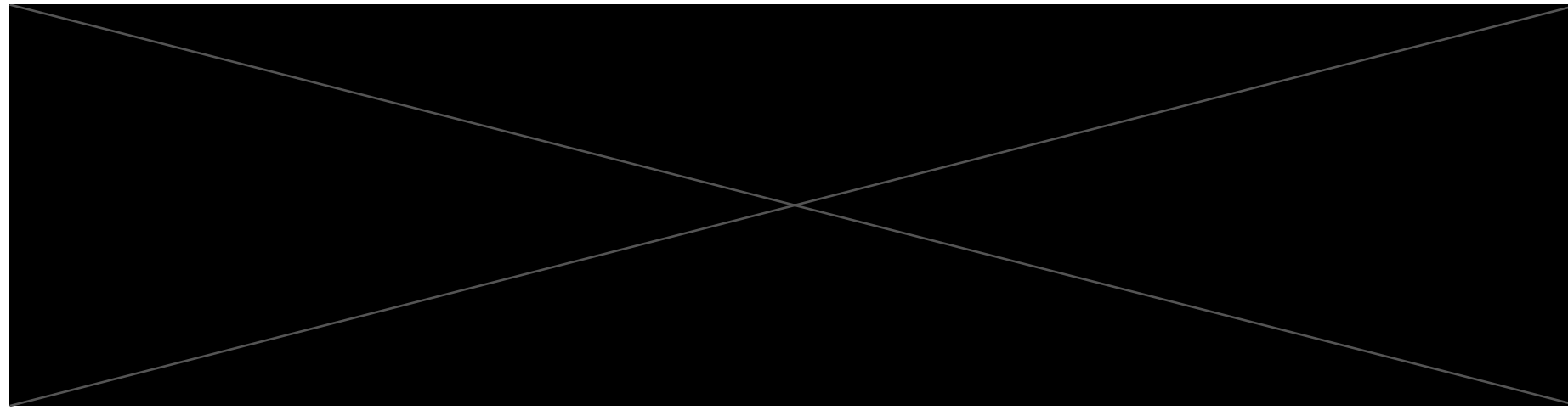
Cybercrime und der Staat

Alternativtitel: Nicht jeder Cocktail ist genießbar



Wer ist das?

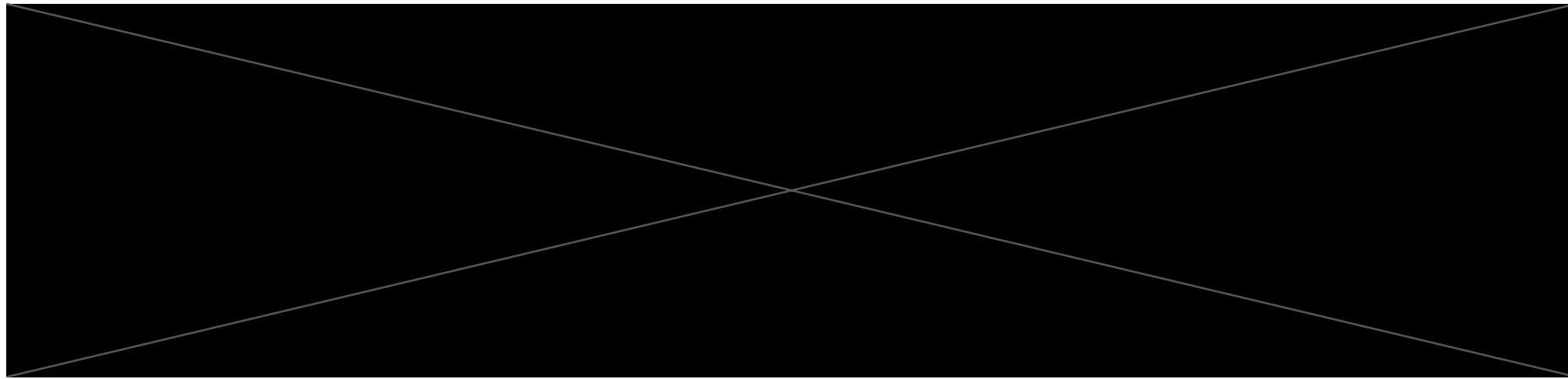
Und warum sollten Sie ihm zuhören?



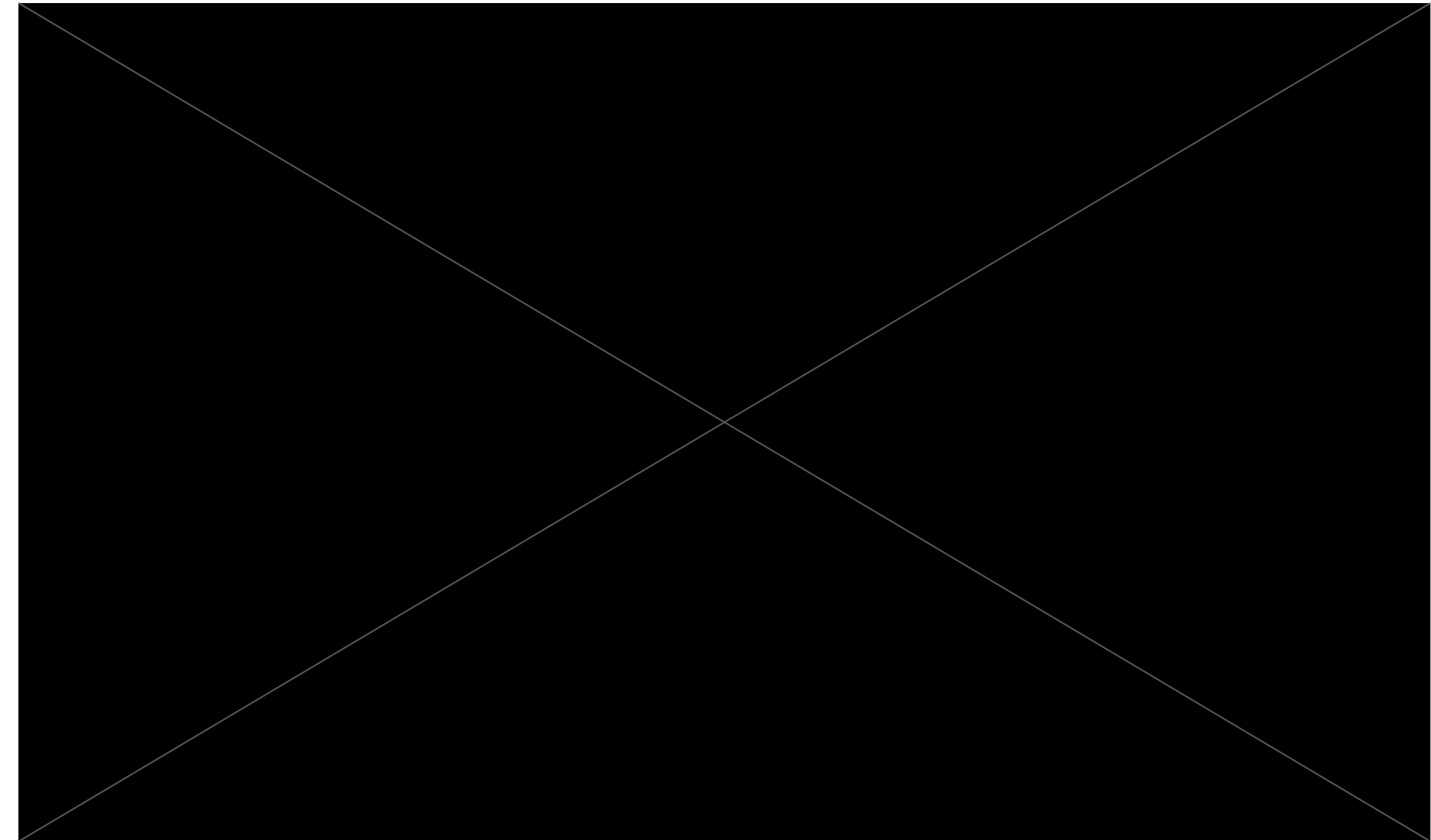
- **Fokus auf strategischer Threat Intelligence**
 - Insbesondere: Auswirkungen von Geopolitik
 - Ich bin ein toller Partygast!

Wer ist das?

Und warum sollten Sie ihm zuhören?

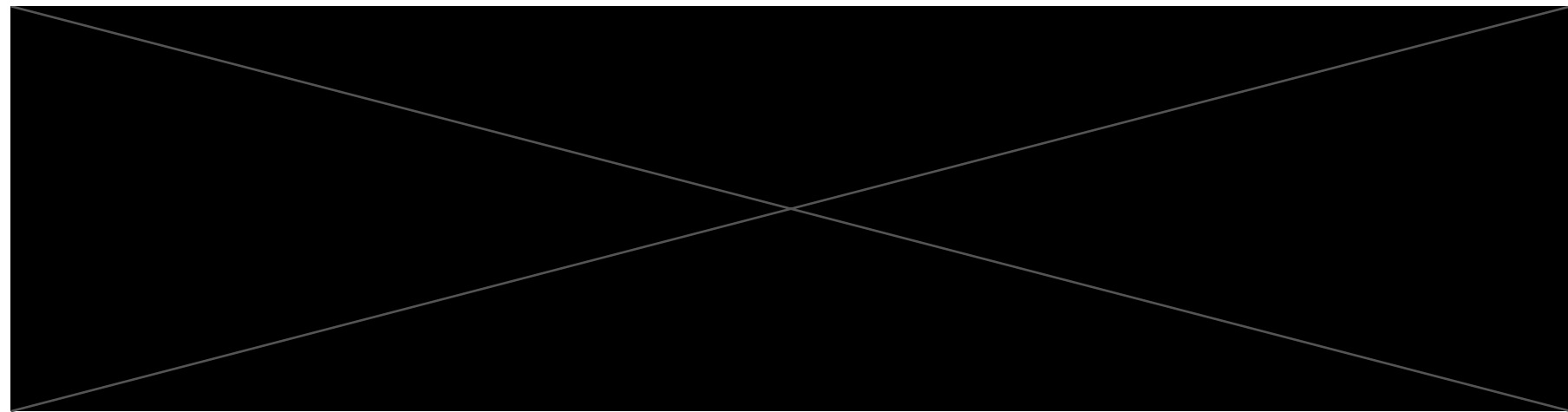


- **Fokus auf strategischer Threat Intelligence**
 - Insbesondere: Auswirkungen von Geopolitik
 - Ich bin ein toller Partygast!

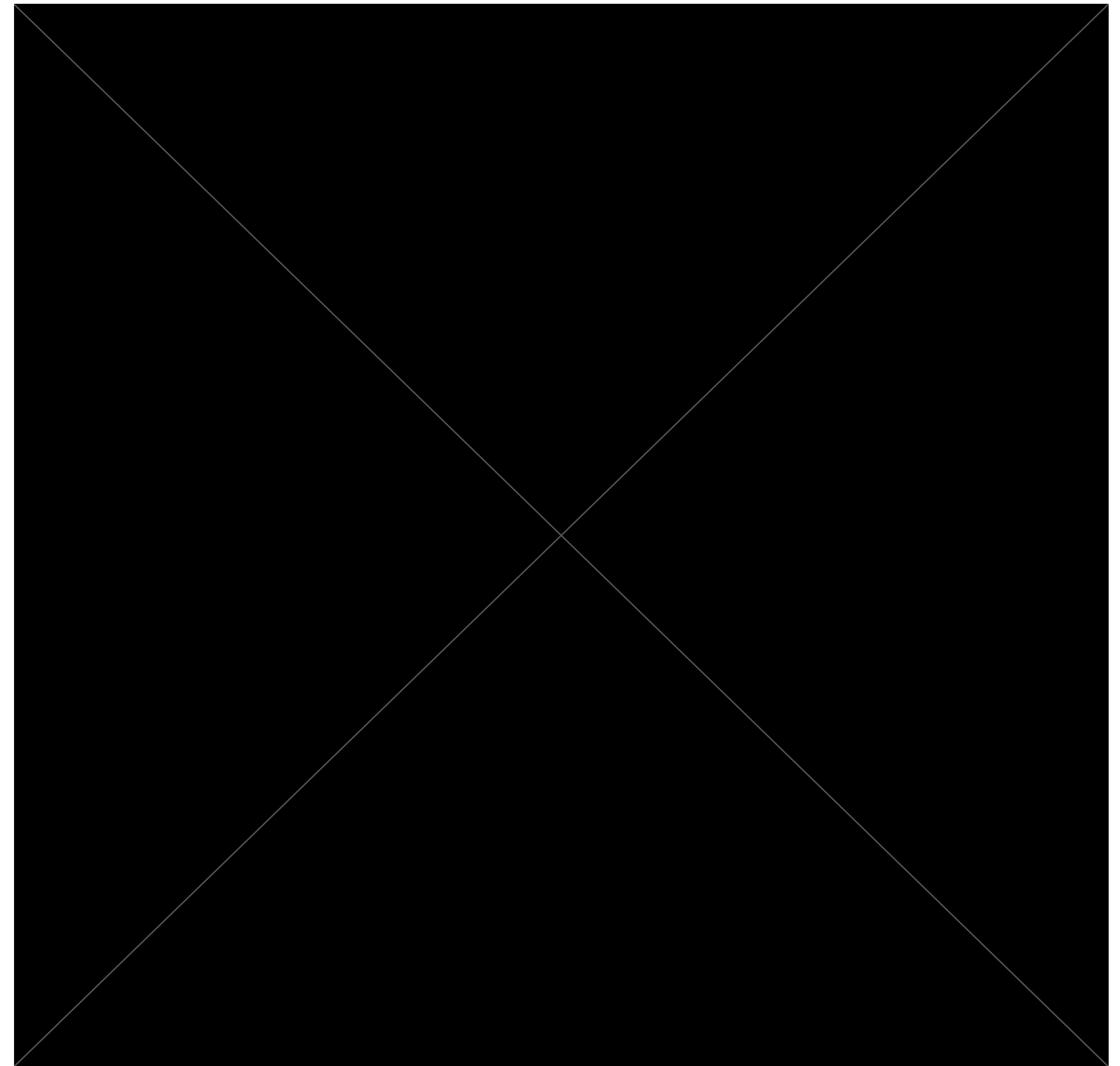


Wer ist das?

Und warum sollten Sie ihm zuhören?

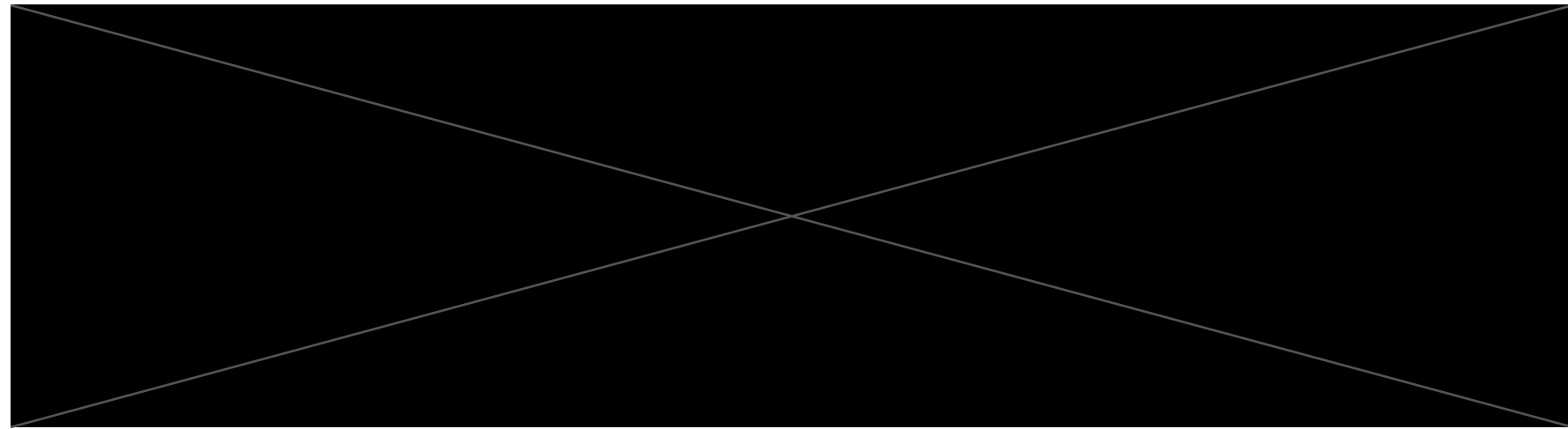


- **Fokus auf strategischer Threat Intelligence**
 - Insbesondere: Auswirkungen von Geopolitik
 - Ich bin ein toller Partygast!



Wer ist das?

Und warum sollten Sie ihm zuhören?



- **Fokus auf strategischer Threat Intelligenc**
 - Insbesondere: Auswirkungen von Geopolitik
 - Ich bin ein toller Partygast!

Ein Bedrohungsakteur kompromittiert
hunderte Unternehmen aus finanziellen
Motiven.

Ein Bedrohungsakteur kompromittiert hunderte Unternehmen aus finanziellen Motiven.

Teile seiner Infrastruktur hat Überlappungen mit Cyberspionage die staatlichen Akteuren zugerechnet wird.

Cybercrime? Spionage?
Staatlich? Kriminell? Alles davon?

Es ist kompliziert ..

.. wer hätte das gedacht.

- **Damals: Script Kiddies, Hacktivisten, Cybercrime, APT**
 - Bequem, (damals schon) unzureichend
- **Heute:** Bedrohungsakteure
 - Fließende Grenzen, mehrfache "Mitgliedschaften"
- **(Noch anhaltende) Entwicklung über Jahrzehnte hinweg**
 - Graduelle Entwicklung auf parallelen "Pfaden"

Macht aber eigentlich Sinn ..

- **Plausible Abstreitbarkeit von Cyberangriffen**
 - Gleichzeitig: Probates Mittel in nicht-kinetischen Konflikten sein
- **Zugriff auf Talente außerhalb formaler staatlicher Strukturen**
 - Kann günstiger sein, kann vor allem aber mehr Kapazitäten ermöglichen
- **Möglichkeit potentiell signifikante Mengen an Geld zu “verdienen”**

Entwicklungen - Extern

Nützliche Aussenseiter

- **1986: Westdeutsche Hacker verkaufen Informationen an den KGB**
- **1990er: Aufstieg krimineller Märkte**
 - Hohe Bildung, wenig Chancen auf dem Arbeitsmarkt, schwache Behörden
- **1998: Patriotischer Hacktivismus**
 - Staatliche Ermunterung, z.B. "Honker Union" in China

Entwicklungen - Intern

“Das können wir auch selbst”

- **1998: Gründung des “Büro 121” in Nordkorea**
 - Grundstein für finanziell motivierte Cyberangriffe ~15 Jahre später
- **2002: FSB lobt (und rekrutiert) Studenten die “feindliche” Webseiten angreifen**
 - Beginn des Aufbaus offensiver Cyberkapazitäten
- **2010: MSS rekrutiert erstmals gezielt ehemalige Hacker**
 - Studenten der “Honker Union” haben inzwischen Jobs

Unterschiedliche Staaten,
unterschiedliche Systeme.

#1: RF



Ich hab ein Крыша, ein kunterbuntes Крыша, .. 

- **Fall der Sowjetunion erzeugt ein riesiges kriminelles Ökosystem, on- und offline**
 - Der Staat toleriert profitorientierte Kriminelle - auch im Cyberraum
 - Teilweise mehr als Toleranz -> offene Protektion
- **Diese Toleranz ermöglicht ein gewisses Maß an Kontrolle - und Nutzung**
 - Große Auswahl an kriminellen Täter:innen / Services
 - Wenig Aufwand bei gleichzeitiger Abstreitbarkeit

Evil Corp

(Ich hab ein **Крыша**, ein kunterbuntes **Крыша**, .. 🎵)

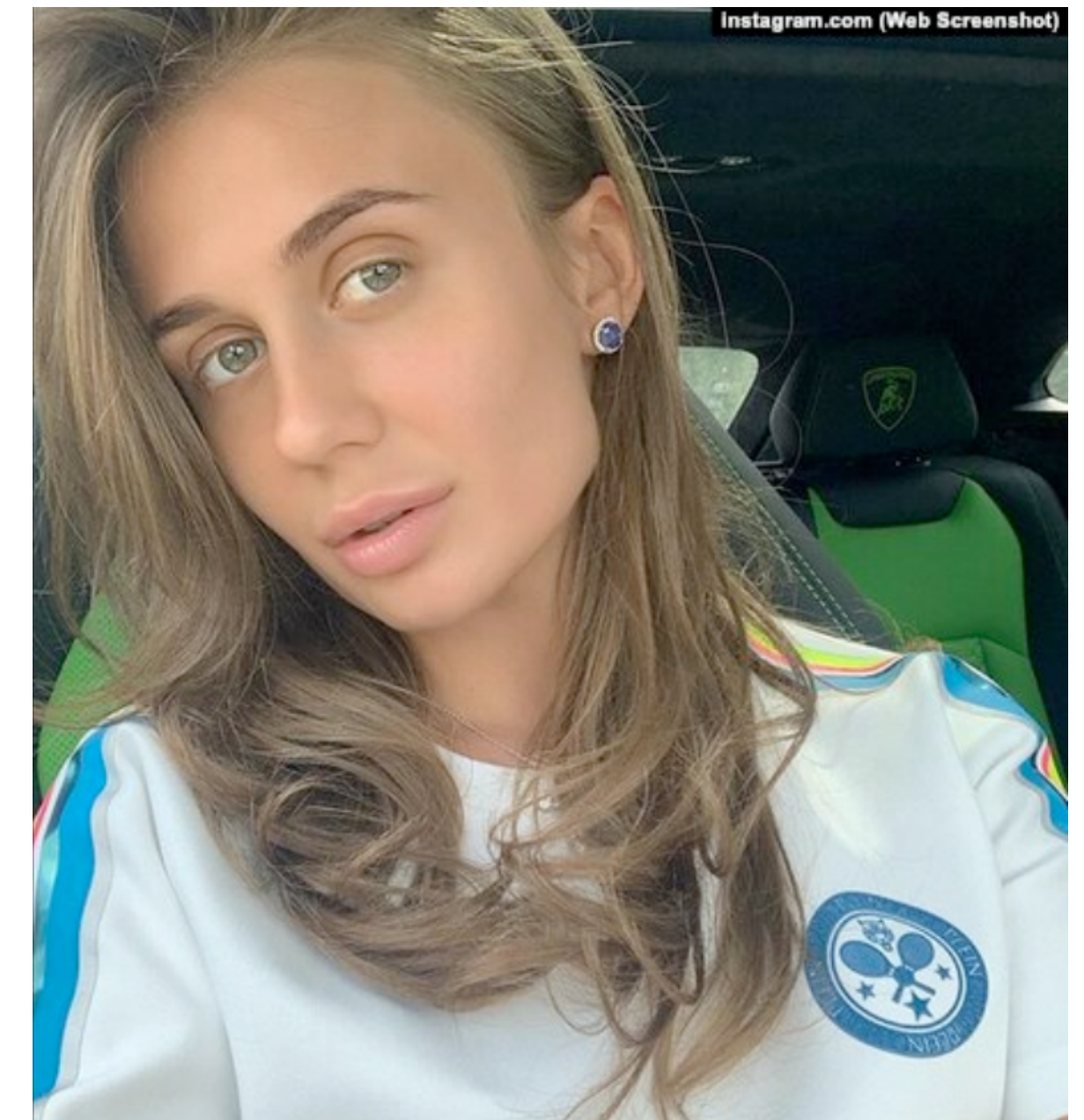
- **Finanziell motivierter Bedrohungsakteur**
 - Über 10 Jahre lang aktiv, Millionenschäden
- **Kernakteur: Maksim Yakubets**
 - Jabber Zeus (2009) -> Evil Corp (2014)
 - Interessantes Privatleben!



Evil Corp

(Ich hab ein **Крыша**, ein kunterbuntes **Крыша**, .. 🎵)

- **Finanziell motivierter Bedrohungsakteur**
 - Über 10 Jahre lang aktiv, Millionenschäden
- **Kernakteur: Maksim Yakubets**
 - Jabber Zeus (2009) -> Evil Corp (2014)
 - Interessantes Privatleben!









Evil Corp

Ich hab ein **Крыша**, ein kunterbuntes **Крыша**, .. 🎵

- **Eduard Bandersky**
 - Ehemals KGB, Vympel
 - Heute "Privatier"
- **Ein Schelm wer böse Dinge denkt ..**
 - Teilweise interessante "Ausreißer" bei Evil Corp



Evil Corp

Mein **Крыша** brennt!

- Befindlichkeiten sind selbstverständlich
- Direktion K des FSB interessiert/e sich für Evil Corp
- G(R)U hat auch Interesse gezeigt



#2: DPRK



Staatliche Kriminalität

Von Disruption zu Gewinn

- **Zentrale staatliche Stelle für “Cyberkrieg”, Bureau 121**
- **Anfangs primär disruptive Aktivitäten**
 - DDoS-Angriffe 2009, Sony-Hack in 2014
- **Seit ungefähr 2015:** 💰💰💰💰💰
 - Angriffe gegen Banken und SWIFT, später auf Kryptowährungen
- **Inzwischen eingespielte Taktiken, aber immer wieder neue Innovationen**

2025: Über 3 Milliarden
gestohlene Dollar

#3: CN

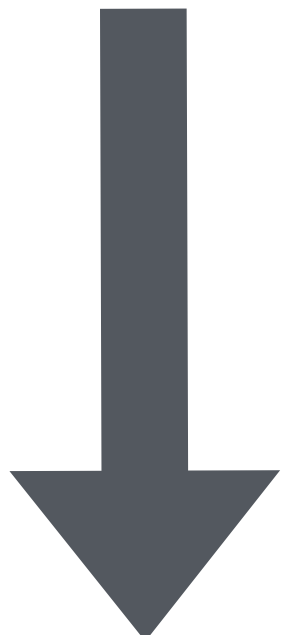


Chinesische Regierung

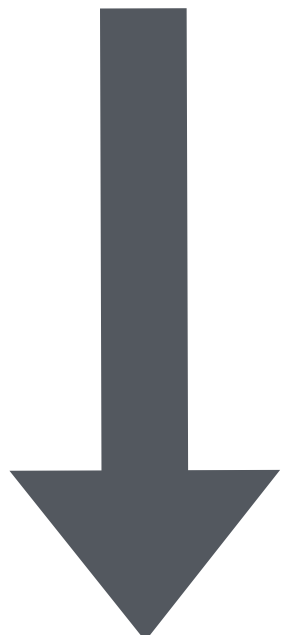


Chinesische Hacker

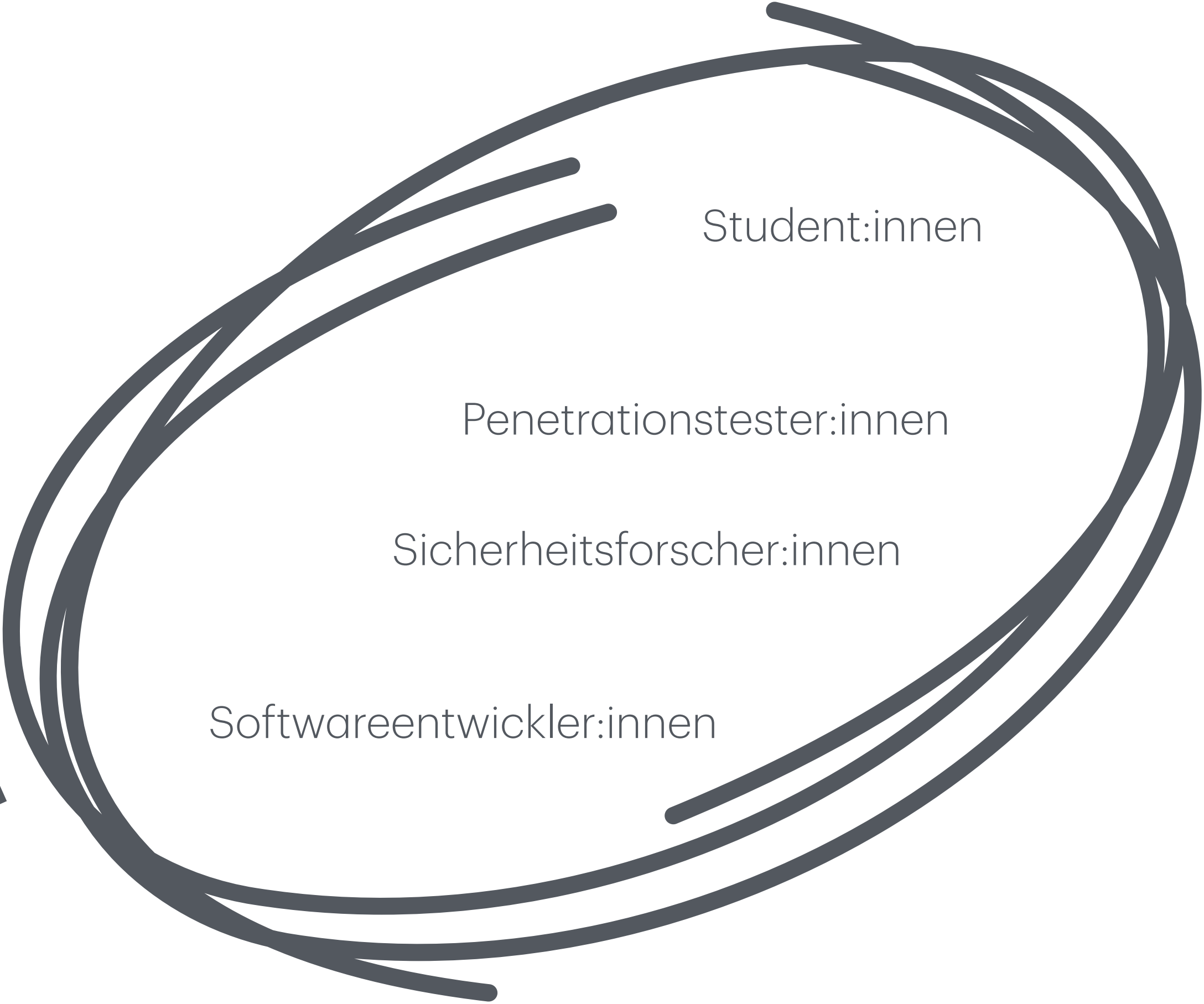
Chinesische Regierungsorganisationen



Chinesische Unternehmen



Cyberangriffe



Student:innen

Penetrationstester:innen

Sicherheitsforscher:innen

Softwareentwickler:innen

Es lebe das Chaos!

我工作量过大，但薪水过低.

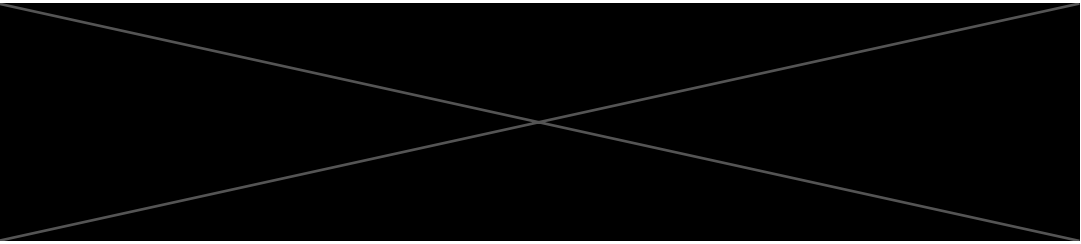
- **MSS und PLA haben sehr lange vollständig eigenständig agiert**
 - 2010: Erstmaliges Involvieren von "Aussenseitern"
- **Teilweise sehr unterschiedliche Arrangements**
 - 2012: Klassische Spionage 🤝 finanzielles Eigeninteresse
- **Inzwischen vollständige Integration von privaten Akteuren**
 - Sowohl "legitime" Firmen als auch cyberkriminelle Strukturen

Was bedeutet das also?

Und was können wir dagegen tun?

- **Attribuierung wird (noch) schwieriger**
 - Technisch, vor allem aber politisch / juristisch
- **Zusammenarbeit von Institutionen wichtiger als je zuvor**
 - Strafverfolger, Nachrichtendienste, Diplomaten
- **Kriminelle Ökosysteme bekommen eine neue Bedeutung**
 - Infrastruktur, Malware-Entwickler:innen, Access Broker, ..

Vielen Dank für Ihre Aufmerksamkeit

- Bei Kritik, Beschwerden, Unmutsäußerungen 
- Bei Fragen, Anregungen, gut dotierten Jobangebote 