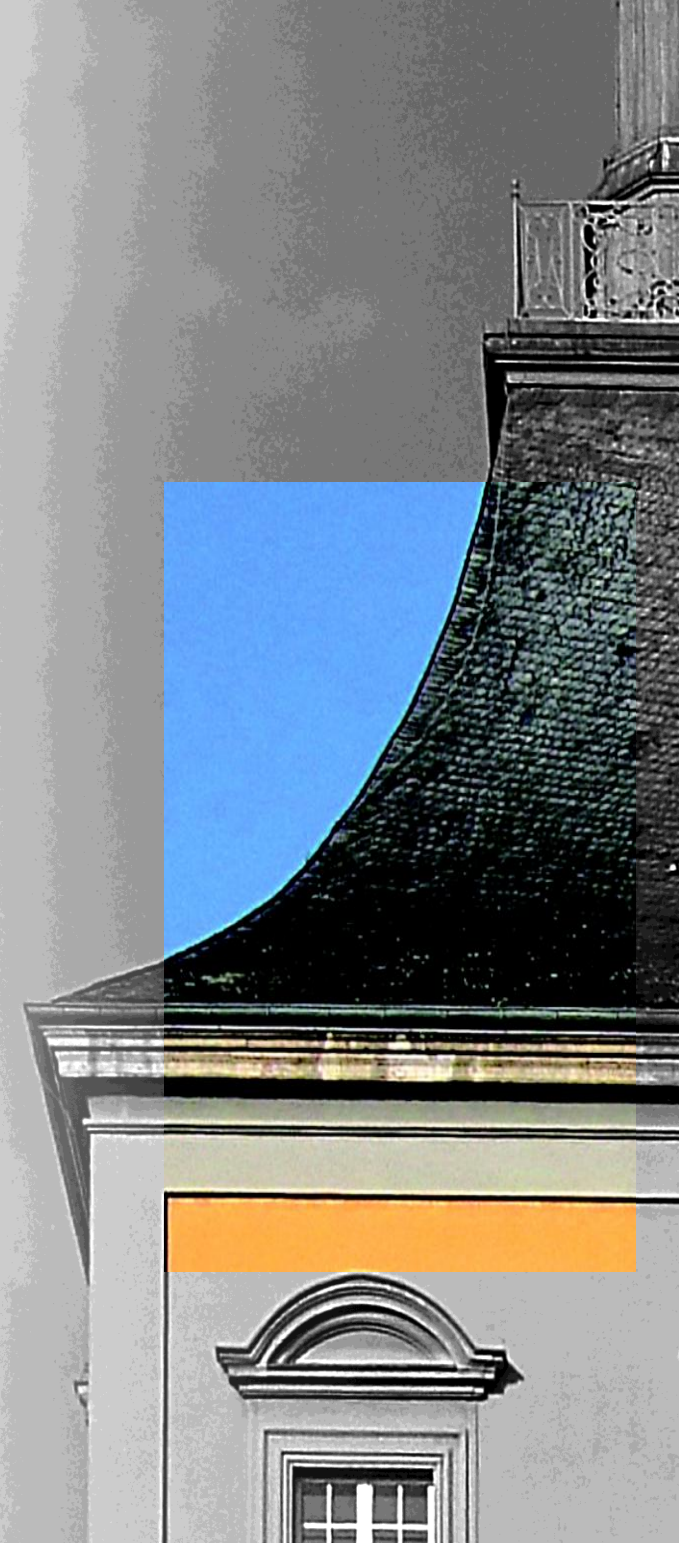


VORLESUNG  
NETZWERKSICHERHEIT

***SOMMERSEMESTER 2023***  
***MO. 14-16 UHR***



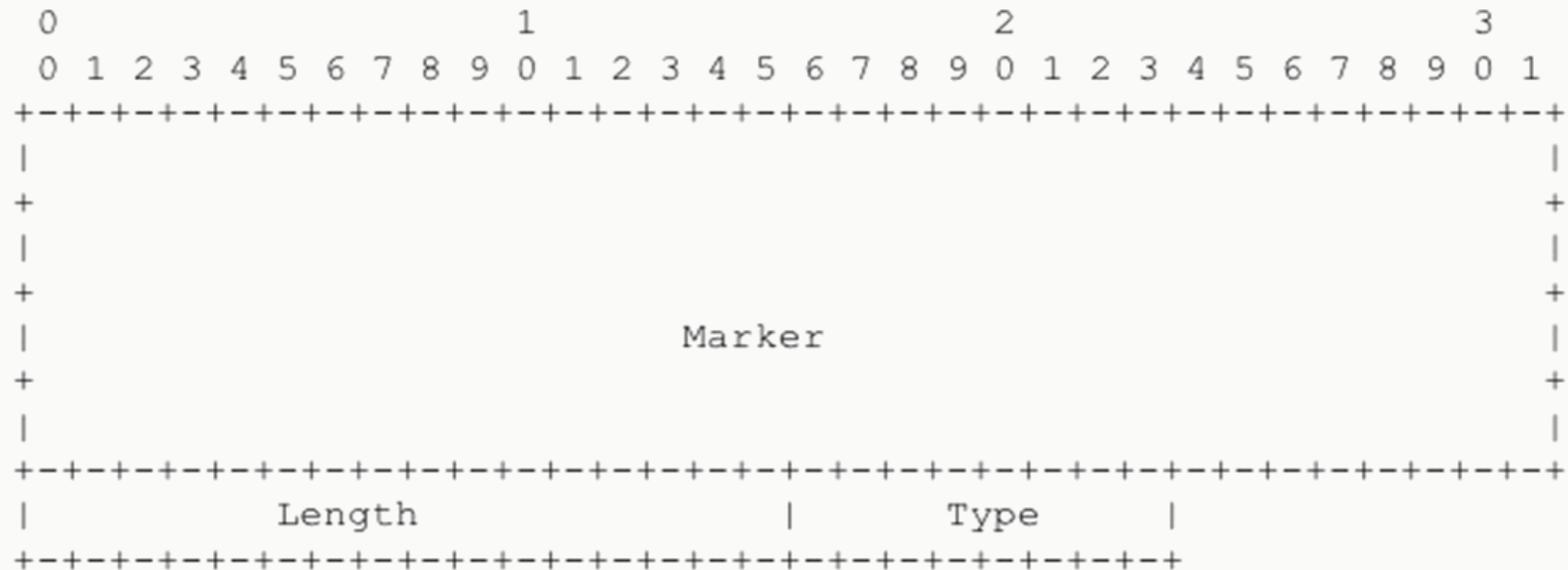
## KAPITEL 4

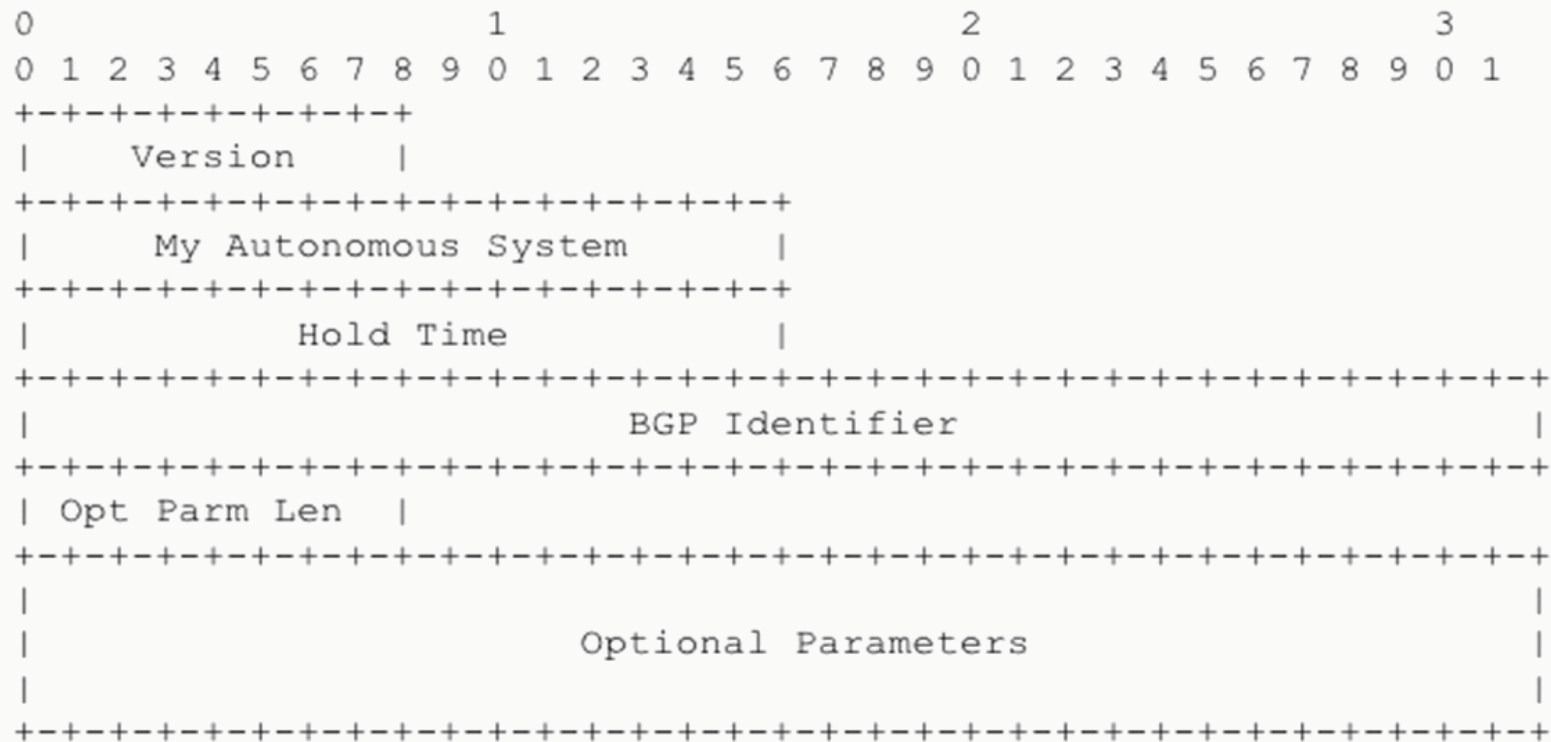
# ***INTERNET ROUTING (ANOMALIEERKENNUNG)***

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological Disorder
  - Angriffsszenario “Quantuminsert”
- Prefix-Hijacking
- Analyse von Routinganomalien

# ROUTINGANOMALIEN – BORDER GATEWAY PROTOCOL

## BGP (v4)-Header:

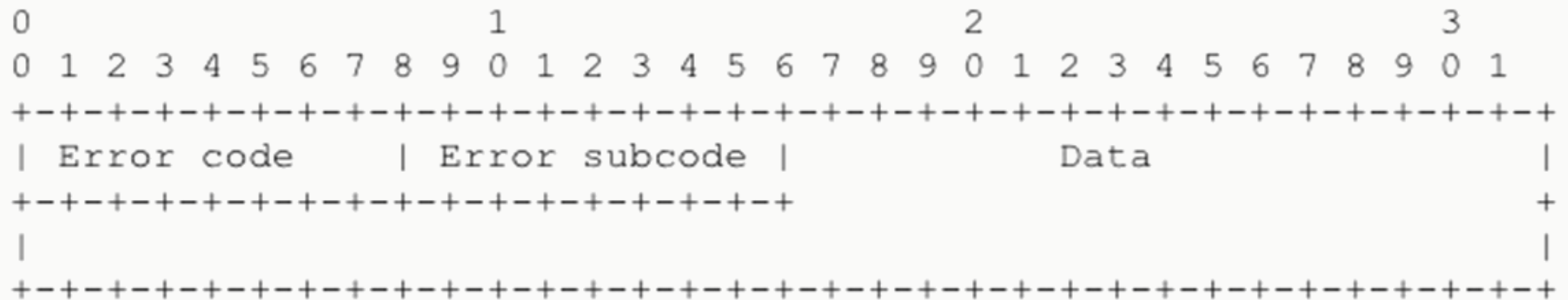




[illegible]

# ROUTINGANOMALIEN – BORDER GATEWAY PROTOCOL

## BGP Notification:



### ■ Error codes:

- 1: HARD Error
- 2: OPEN Error
- 3: UPDATE Error
- 4: Hold Time Expired
- 5: FSM Error
- 6: Cease (unspecified fatal error)

# ROUTINGANOMALIEN – BORDER GATEWAY PROTOCOL

## BGP Update Message:

```

+-----+
|   Unfeasible Routes Length (2 octets)   |
+-----+
|   Withdrawn Routes (variable)           |
+-----+
|   Total Path Attribute Length (2 octets) |
+-----+
|   Path Attributes (variable)             |
+-----+
|   Network Layer Reachability Information (variable) |
+-----+

```

### ■ Path Attributes:

```

0           1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Attr. Flags |Attr. Type Code|
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

### ■ NLRI:

```

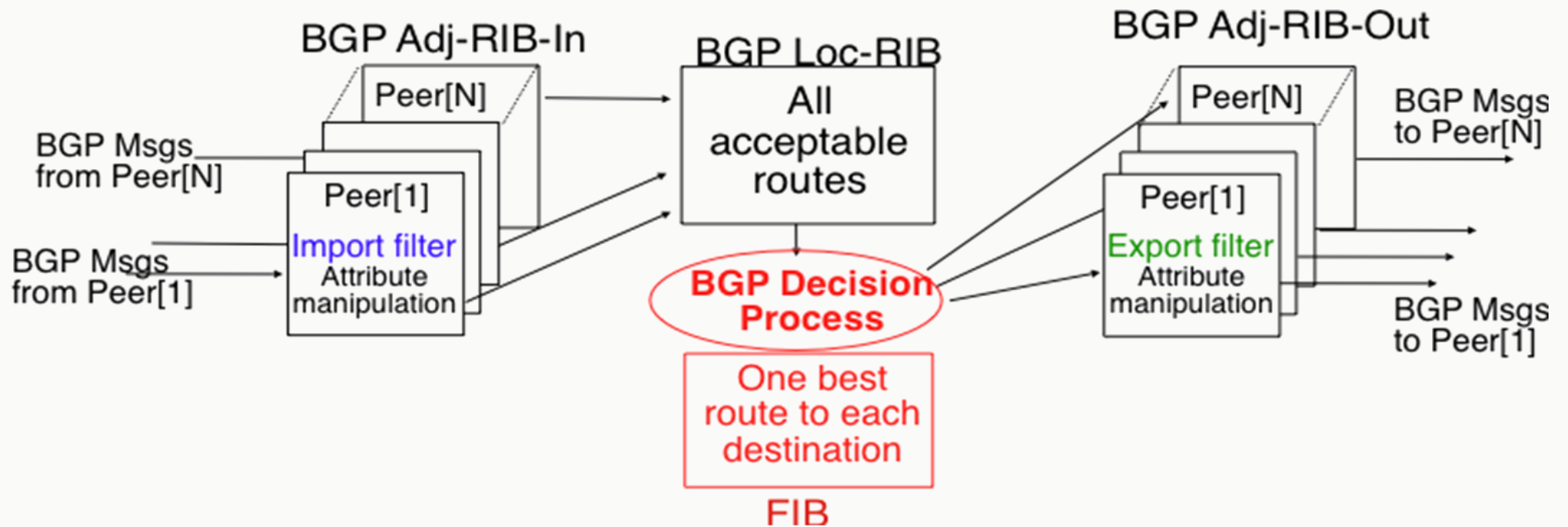
+-----+
|   Length (1 octet)   |
+-----+
|   Prefix (variable)  |
+-----+

```



# ROUTINGANOMALIEN – BORDER GATEWAY PROTOCOL

## ■ Routen-Verarbeitung



Aus Computer Networking : Principles, Protocols and Practice 2<sup>nd</sup> Ed.

## Routen-Auswahl-Algorithmus (“Best Practice”)

1. Benutzer-Richtlinien (Policies) zur Anpassung von Variablen
2. Wähle die Route mit der größten Local-Preference (policy, AS intern)
3. Wähle die Route mit dem kürzesten Pfad (dynamisch)
4. Wähle die Route mit dem kleinsten MED (bei Routen vom selben AS erzwungen)
5. “Tie-Breaking”:
  1. Wähle die Route mit dem kleinsten MED (falls nicht bereits in Stufe 4)
  2. Wähle die Route mit den geringsten Kosten / Metric für den nächsten Hop (basiert auf dem genutzten Interior-Gateway-Protocol)
  3. Wähle die Route des externen BGP-Peers mit der kleinsten IP-Adresse als BGP-Identifizier
  4. Wähle die Route des internen BGP-Peers mit der kleinsten IP-Adresse als BGP-Identifizier

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological Disorder
  - Angriffsszenario “Quantuminsert”
- Prefix-Hijacking
- Analyse von Routinganomalien

## Der Begriff "Routinganomalie"

- In diesem Kontext: Anomalie in Bezug auf das Border Gateway Protocol (BGP v4).

## Ursachen für Routinganomalien

- Angriffe
- Fehlkonfiguration
- Software-Bugs

## Unterscheidung der Routinganomalien in zwei Arten

- Topological-Disorder
- Prefix-Hijacking

## (Historische) BGP-Angriffsvektoren

- BGP-Nachrichten sind normaler Inter-AS-Datentransfer
  - BGP-Sessions sind öffentliche Dienste, jeder kann sich verbinden.
  - Lösung: Gegenseitige Authentifikation von BGP-Peers mit einem "Passwort".
- BGP bietet keine Überprüfung der Announcements (NLRI)
  - Gegenseitiges Vertrauen zwischen Peers führt zu einem transitiven Vertrauen:
    - Relation R: "trust"
    - Sei:  $1R2, 2R3$  (= AS 1 vertraut AS 2, AS 2 vertraut AS 3)
    - $\Rightarrow 1R3$  (= AS 1 vertraut AS 3)
  - Lösung: (Kryptographische) Signatur von Announcements (in jedem AS-Hop)
- BGP bietet keine Ursprungs-Verifikation
  - Es gibt keine zuverlässige Zuordnung von IP Prefix  $\Rightarrow$  AS #
  - Lösung: (Kryptographische) Signatur des Ursprungs-AS (RPKI)

# *ROUTINGANOMALIEN – ANGRIFFSVEKTOREN & ANGREIFERMODEL*

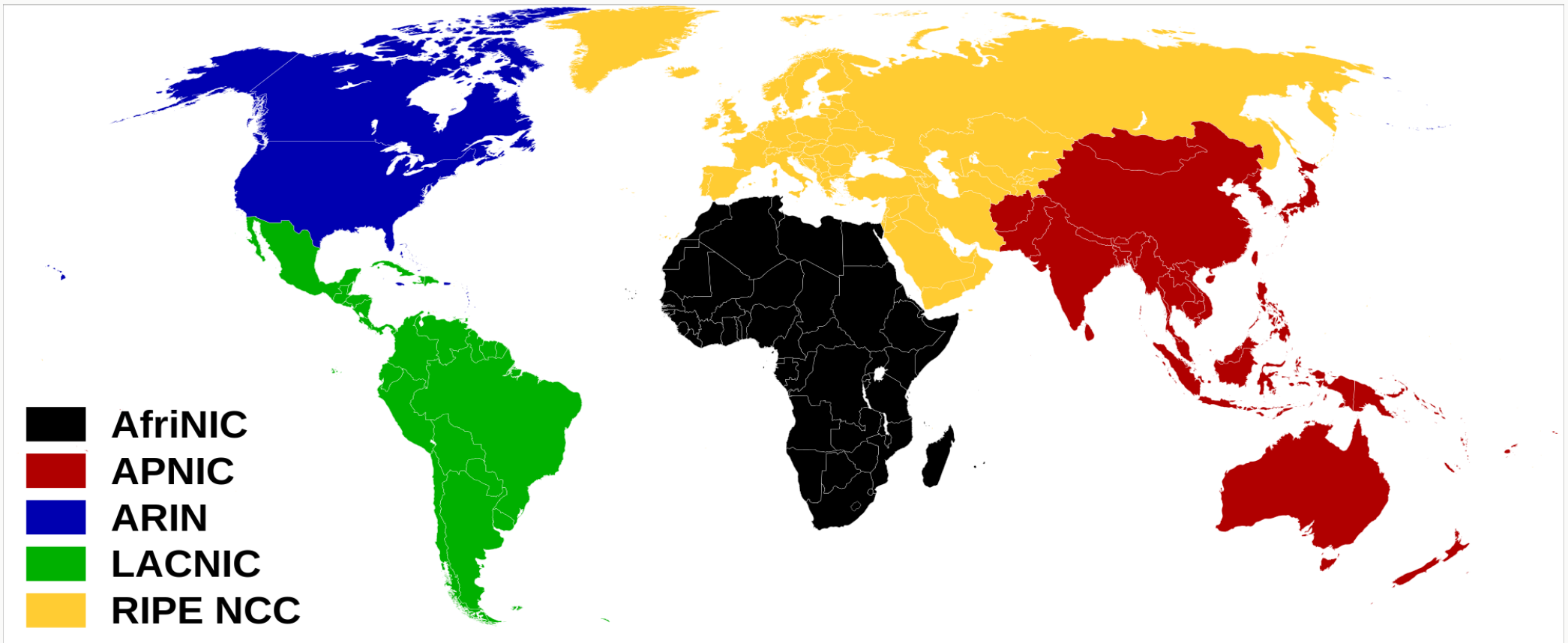
Ein resultierendes Angreifermodell:

- Historisch: Jeder!
- Derzeit: Registrierte AS oder Netzwerke, die an “schwache” AS angebunden sind
- Zukünftig: Wer kryptografische Signaturen brechen kann

Wie wird man Teil des Internets?

- Registriere eine AS-Nummer bei der verantwortlichen RIR
  - RIR = Regional Internet Registry

- Wie wird man Teil des Internets?







- Wie wird man Teil des Internets?
  - Registriere eine AS-Nummer bei der verantwortlichen RIR
    - RIR = Regional Internet Registry
    - Whois-Informationen werden vom registrierten AS selbst verwaltet
  - Erlange einen IP-Prefix, um aus dem Internet erreichbar zu sein
    - Option 1: Bewerbung um freie IP-Prefixe beim RIR
    - Option 2: Kauf eines IP-Prefix von einem anderen AS
    - Option 3: Kauf/Übernahme des Betreibers eines anderen AS, Übertrag von IP-Prefixen, Verkauf des Betreibers mit weniger IP-Prefixen.
  - Hinweis für Optionen 2 und 3: die RIR muss nicht über den Besitzerwechsel des IP-Prefixes informiert werden



Wie wird man Teil des Internets?

- Aufbau von Verbindungen zu anderen AS (peering)
  - Upstream (bezahlter Provider)
  - Peer (üblicherweise nicht bezahlt, aber: gegenseitiges Einverständnis, meist über einen Vertrag abgesichert)
- Ankündigung des eigenen Prefixes

RPKI = Resource Public Key Infrastructure

- Der Prefix ist die Ressource
- RIR ist Zertifikat-Authorität (CA)

Sicheres Internetrouting mit RPKI?

- Legitime Besitzer von Prefixen benötigen einen ROA von ihrer RIR.
- ROA (Route Origin Authorization), ein kryptografisches Zertifikat.
- Jedes Announcement enthält die ROA.

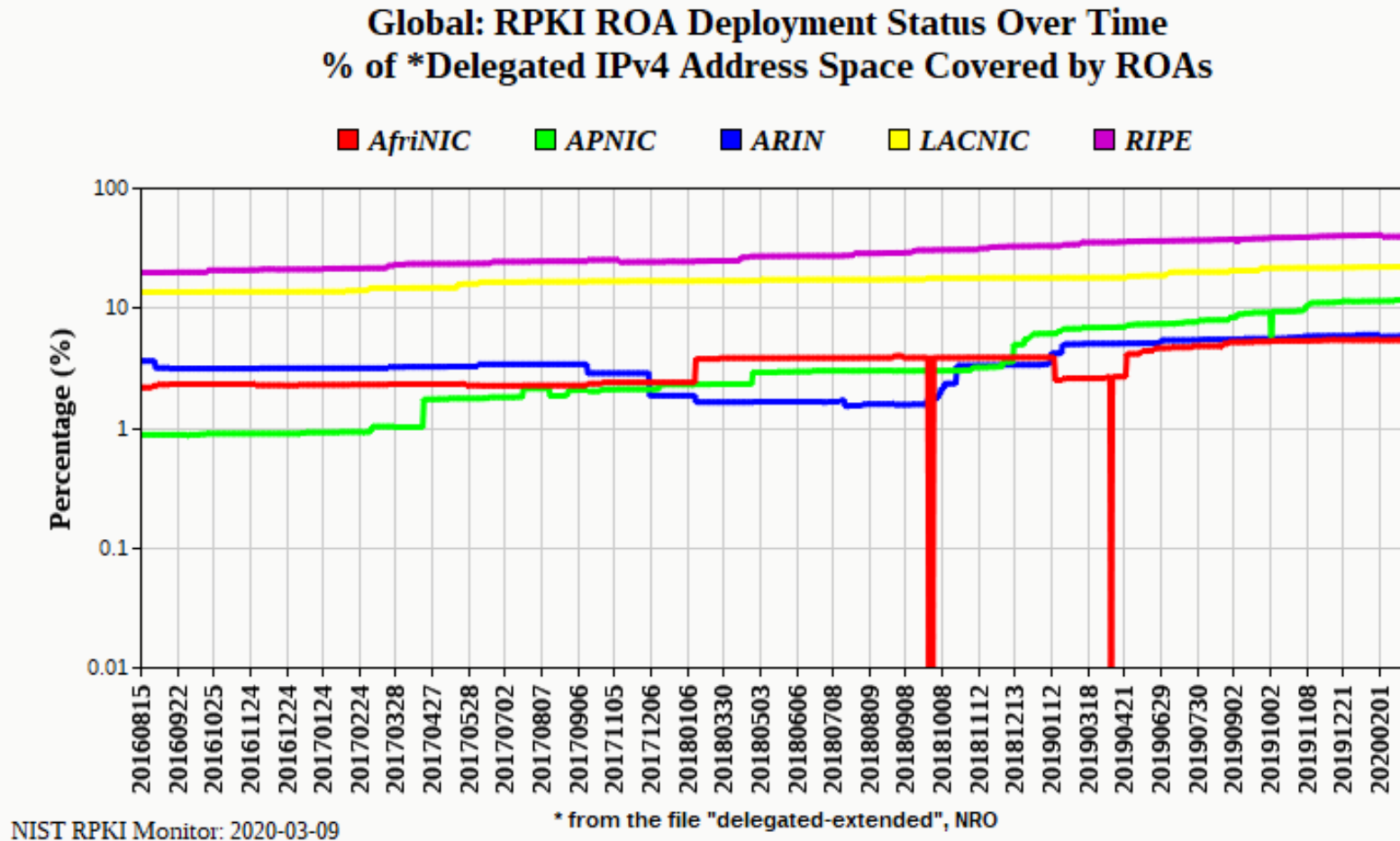
Zukünftig:

- Das Internetrouting wird mehr und mehr durch RPKI abgesichert

Probleme:

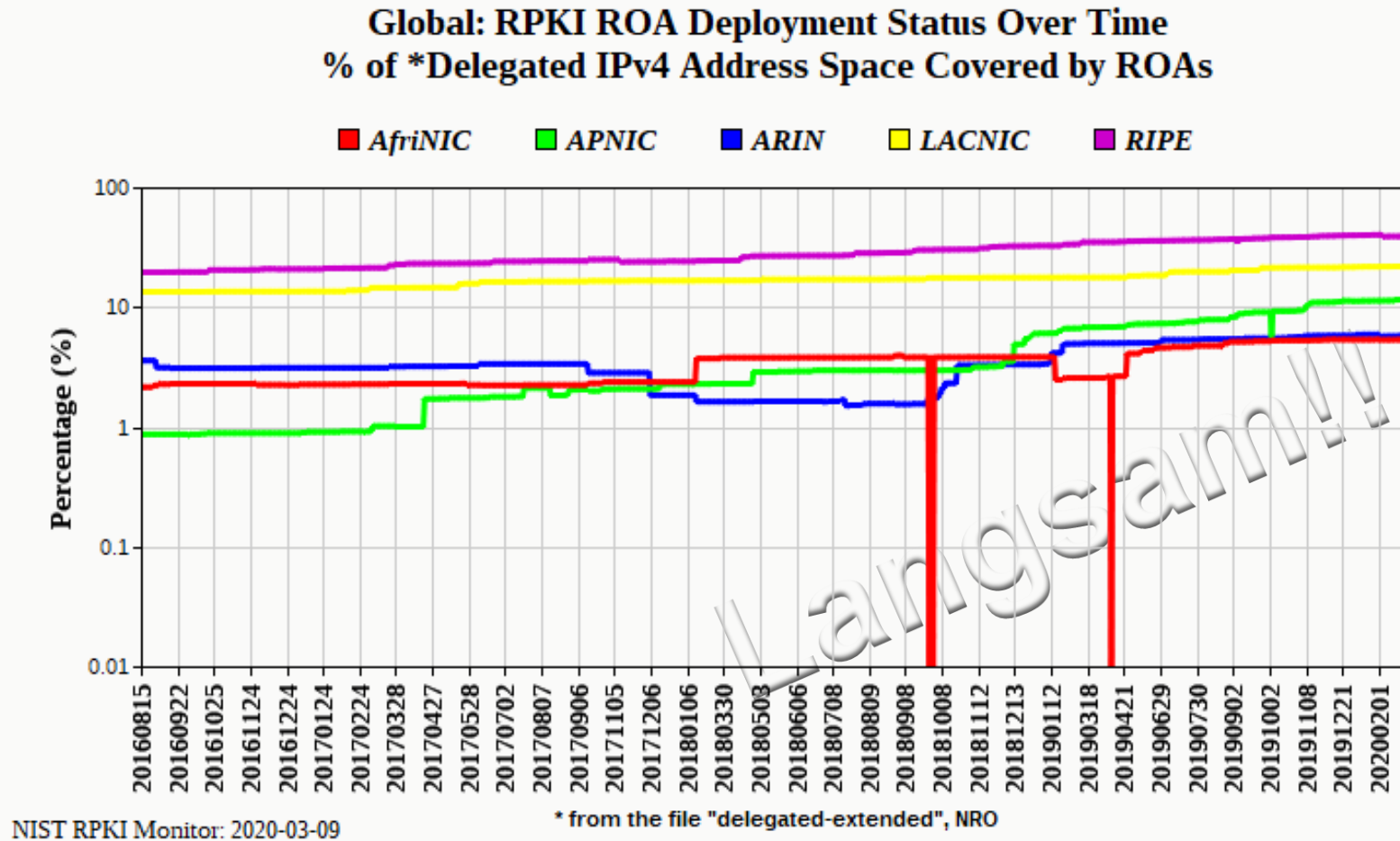
- (Kurzfristig) Übliche Routing-Hardware nicht für "viel" Kryptografie ausgelegt
- (Langfristig) Übliche "State-Actor" können auch RIRs kontrollieren

# ROUTING ANOMALIES – ATTACK VECTORS (II) – RPKI



<http://rpki-monitor.antd.nist.gov/?p=0&s=1> – aus März 2020, Statistik so nicht mehr verfügbar!

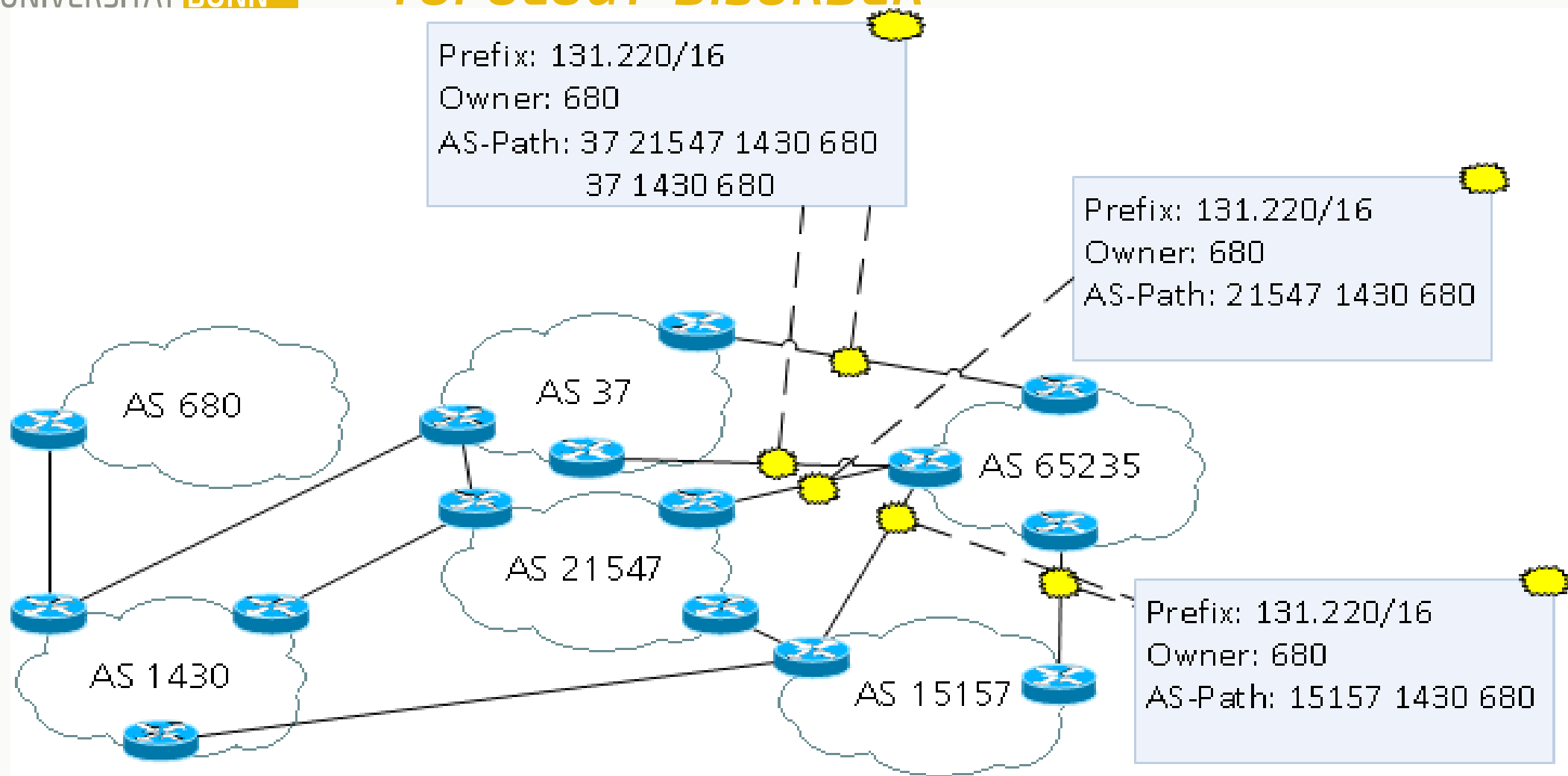
# ROUTING ANOMALIES – ATTACK VECTORS (II) – RPKI



<http://rpki-monitor.antd.nist.gov/?p=0&s=1> – aus März 2020, Statistik so nicht mehr verfügbar

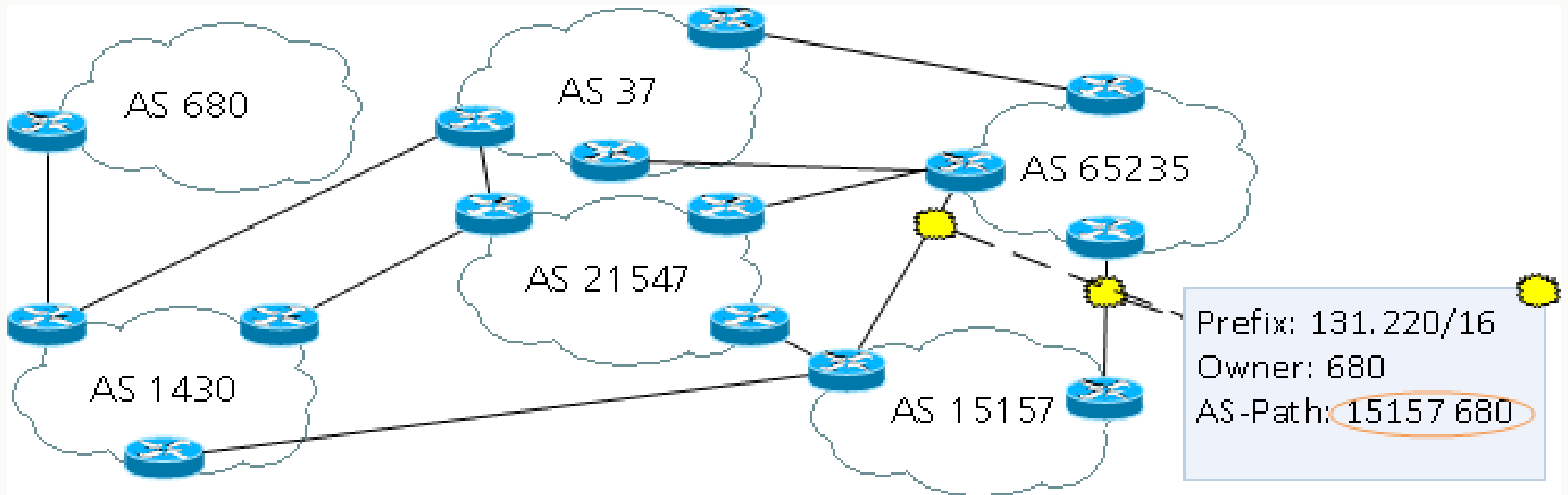
- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological Disorder
  - Angriffsszenario “Quantuminsert”
- Prefix-Hijacking
- Analyse von Routinganomalien

# ROUTINGANOMALIEN – TOPOLOGY-DISORDER



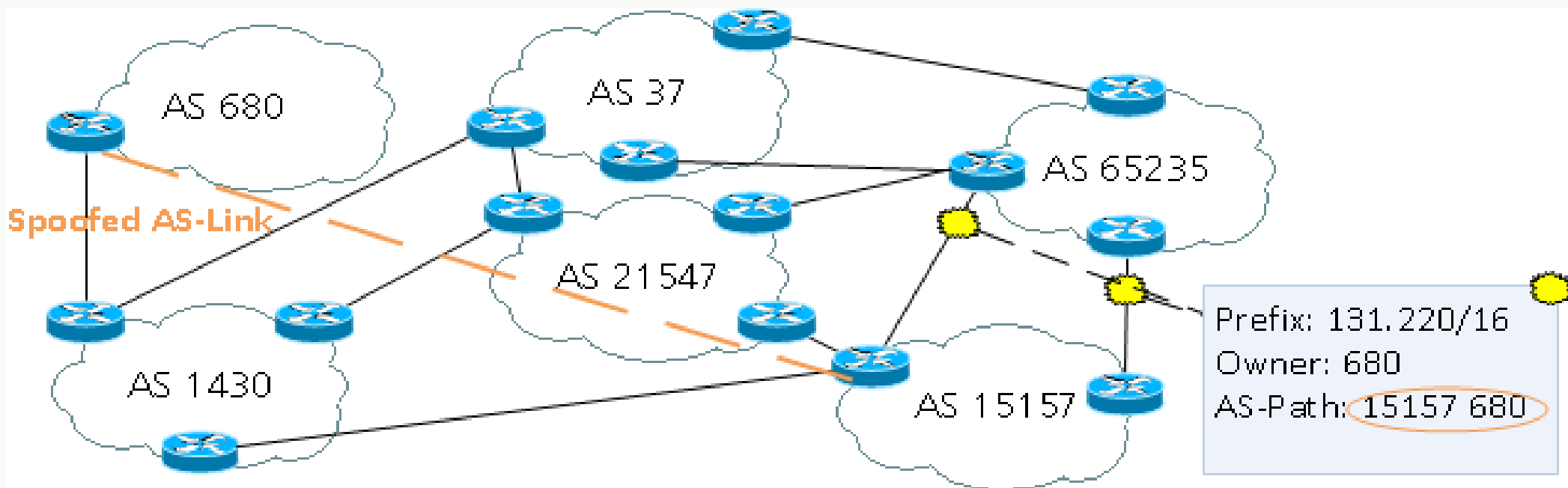
# ROUTINGANOMALIEN – TOPOLOGY-DISORDER

Annahme: AS 15157 ist Angreifer (und möchte Datenverkehr abgreifen)





Annahme: AS 15157 ist Angreifer (and möchte Datenverkehr abgreifen)



## Varianten der Pfadmanipulation in einem Announcement

- Pfad-Verkürzung / Entfernte AS hops
  - Führt zu kürzeren AS-Pfaden (im Announcement)
  - Opfer-AS folgen (wahrscheinlich) dem kürzeren Pfad
  - Angreifer-AS ist im Pfad als “Man-in-the-Middle”
  
- Pfad-Verlängerung
  - Führt zu längeren Pfaden (im Announcement)
  - Opfer-AS folgen (wahrscheinlich) einem anderen Pfad
  - Angreifer-AS benötigt einen Komplizen auf dem dann gewählten Pfad
    - Diese Technik wird auch von AS genutzt, um Datenverkehr fernzuhalten

## Varianten der Pfadmanipulation in einem Announcement

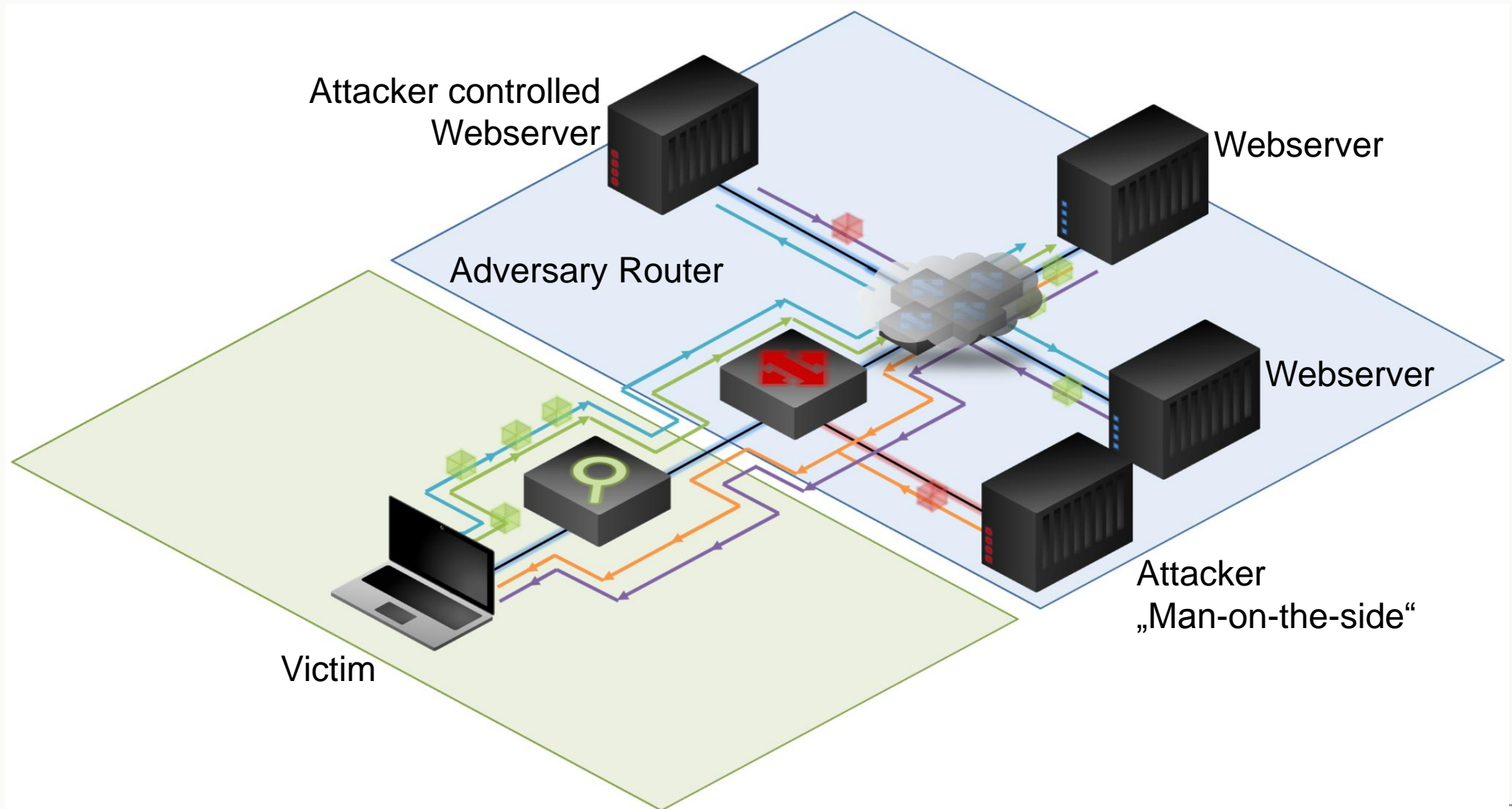
- AS-Hop-Tausch
  - Austausch eines AS im Pfad mit einem anderen AS
  - Kann Datenverkehr auf einen bestimmten Pfad führen (wegen Policies)
  - Möglicherweise weniger auffällig als Pfad-Verkürzung

# ***ROUTINGANOMALIEN – TOPOLOGY-DISORDER - EXKURS***

Annahme: AS 15157 ist Angreifer (und möchte Datenverkehr abgreifen)

- Ist dies ein realistisches Szenario (= eine echte Bedrohung)?

# ROUTINGANOMALIEN – TOPOLOGY-DISORDER - EXKURS



# ROUTINGANOMALIEN – TOPOLOGY-DISORDER - EXKURS

Attacker controlled  
Webserver

Webserver

**Angriff ermöglicht TCP-Spoofing**

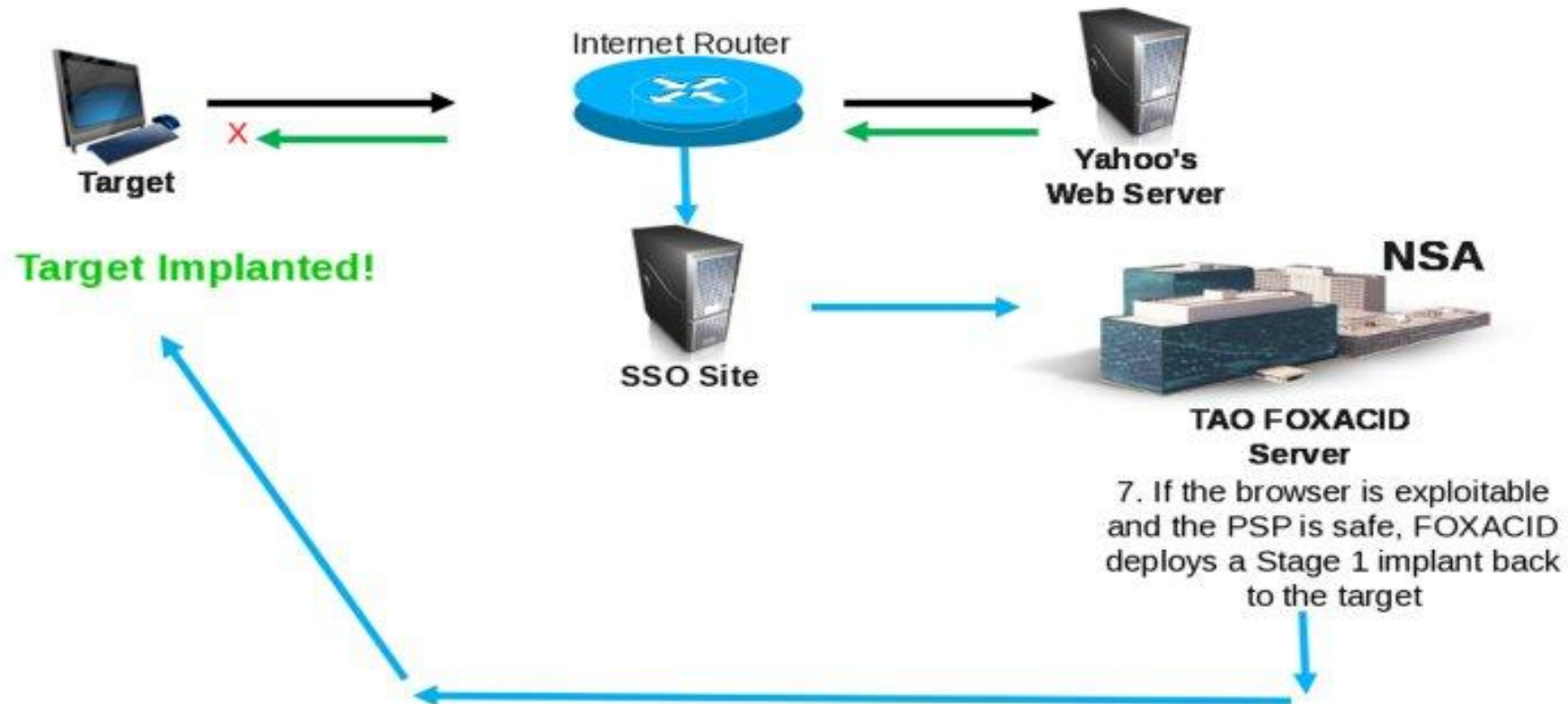
Webserver

Attacker  
„Man-on-the-side“

Victim

# What is QUANTUM?

## QUANTUM Generic Animation – High Level of How It Works




**SDS**

Booz | Allen | Hamilton

SIGINT | Development | Support


# ROUTINGANOMALIEN – ER - EXKURS



Armenian Genocide | The Islamic State | Obama Administration | Yemen | United Nations







ABOUT FP | SUBSCRIBE


NEWS & IDEAS ▾ REGIONS ▾ CHANNELS ▾ GALLERIES ▾ VOICES ▾


 **PASSPORT** Big stories from a small world

## Is the Pirate Bay now hosted in North Korea, or are they messing with us? [Updated]

BY JOSHUA KEATING | MARCH 4, 2013 - 6:34 PM







Visitors to the filesharing megasite Pirate Bay today might be surprised to see a North Korean flag on the page's usual Pirate Ship logo. The image links to the following post on the [site's blog](#):

*The Pirate Bay has been hunted in many countries around the world. Not for illegal activities but being persecuted for beliefs of freedom of information. Today, a new chapter is written in the history of the movement, as well as the history of the internet.*

SHARE •

88 SHARES

Warten auf www.google-analytics.com

22. Mai 2023

Matthias Wübbeling - Vorlesung Netzwerksicherheit - SoSe 2023

32



PASSPORT Big stories from a small world

# Is the Pirate Bay now hosted in North Korea, or are they messing with us? [Updated]

BY JOSHUA KEATING

MARCH 4, 2013 - 6:34 PM



Visitors to the filesharing megasite Pirate Bay today might be surprised to see a North Korean flag on the page's usual Pirate Ship logo. [image links to the following post on the site's blog:](#)

*The Pirate Bay has been hunted in many countries around the world. Not for illegal activities but being persecuted for beliefs of freedom of information. Today, a new chapter is written in the history of the movement, as well as the history of the internet.*

Written auf [www.google-analytics.com](http://www.google-analytics.com)

Topic: Security

Follow via: RSS

## Pirate Bay's 'move' to North Korea a hoax

**Summary:** Following the torrent site's announcement suggesting it was being hosted in North Korea, programmers debunk those claims and believe it had made use of fake routing to hide its true location.



By Ellyne Phneah | March 5, 2013 -- 04:19 GMT (04:19 GMT)

Follow @<http://twitter.com/UpYourElly>

Comments

0

Share on Facebook

more +

The Pirate Bay on Monday announced it moved to a new provider for its Web site, but at least one programmer has found the statement a hoax.

The torrent site had released a [statement on Monday](#) implying it was now being hosted in North Korea, and they had been invited by the leader of the Republic of Korea "to fight their battles from [its] network."

"We believe that being offered our virtual asylum in North Korea is a first step of this country's changing view of access to information," the statement said. "It's a country opening up and one thing is sure, they do not care about threats like we do."

The statement had also after The Norwegian Pirate Party (NPP) released a [pastebin announcement](#) earlier on the same day explaining it was forced to cut the bandwidth they were supplying The Pirate Bay due to financial pressures from the industry.

However, a programmer named Will had found the statement on The Pirate Bay's move to North Korea to be a hoax. In his blog, Will said he backward engineered the signal and traced the actual hosting to a location in Asia, which was not North Korea.

According to his analysis, it is likely the torrent site was hijacking Autonomous System (AS) numbers to hide its true location.

Another analysis on [Hacker News](#) also found The Pirate Bay hijacked some IP addresses, set up a fake Border Gateway Protocol (BGP) advertisement and generated an artificial delay. "They are faking [or] spoofing the ICMP responses. They are also prepending their route advertisement with corresponding AS paths to further disguise it," noted Hacker News.



*The Republic of Korea is actually the official name for South Korea, while the North is known as the Democratic People's Republic of Korea.*

Topics: Security, Korea, Networking



Is t  
in N  
me

BY JOSHUA KE



Written auf [www.noodle-analitics.com](http://www.noodle-analitics.com)

- 3 at-grz-lazg-pe02-vl-2084.upc.at (84.116.229.73) 15.597 ms -> Graz, Austria
- 4 at-vie15a-rd1-vl-2032.aorta.net (84.116.228.85) 18.448 ms -> Vienna, Austria
- 5 de-fra01a-rd3-xe-2-1-0.aorta.net (213.46.160.69) 18.414 ms -> Frankfurt, Germany
- 6 84.116.132.174 (84.116.132.174) 16.739 ms -> Frankfurt, Germany
- 7 xe-0.de-cix.frnkge03.de.bb.gin.ntt.net (80.81.192.46) 82.919 ms -> Frankfurt, Germany
- 8 ae-1.r02.frnkge03.de.bb.gin.ntt.net (129.250.4.163) 21.954 ms -> Frankfurt, Germany
- 9 xe-3-2.r00.dsdfge02.de.bb.gin.ntt.net (129.250.5.61) 20.299 ms -> Frankfurt, Germany
- 10 213.198.77.122 (213.198.77.122) 20.850 ms -> Frankfurt, Germany
- 11 \* \* \*
- 12 xe-0-1-0-3.r02.frnkge03.de.bb.gin.ntt.net (129.250.5.62) 68.594 ms -> Frankfurt, Germany
- 13 xe-0.level3.frnkge03.de.bb.gin.ntt.net (129.250.8.202) 72.588 ms -> Frankfurt, Germany
- 14 vlan90.csw4.Frankfurt1.Level3.net (4.69.154.254) 154.316 ms -> Frankfurt, Germany
- 15 ae-82-82.ebr2.Frankfurt1.Level3.net (4.69.140.25) 152.129 ms -> Frankfurt, Germany
- 16 ae-61-61.csw1.NewYork1.Level3.net (4.69.134.66) 125.457 ms -> New York City, NY, USA
- 17 ae-21-70.car1.NewYork1.Level3.net (4.69.155.67) 127.892 ms -> New York City, NY, USA
- 18 INTELSAT-IN.car1.NewYork1.Level3.net (64.156.82.14) 176.317 ms -> New York City, NY, USA
- 19 209.159.170.215 (209.159.170.215) 199.726 ms -> New York City, NY, USA
- 20 \* 202.72.96.6 (202.72.96.6) 694.793 ms -> **Phenom Penh, Cambodia**
- 21 \* \* 175.45.177.217 (175.45.177.217) 803.654 ms -> **Pyongyang, North Korea**
- 22 -> Dead.

h i - - The Pirate Bay has been hunted in many countries around the world. Not for illegal activities but being persecuted for beliefs of freedom of information. Today, a new chapter is written in the history of the movement, as well as the history of the internet.

Al - actual hosting to a location in Asia, which was not North Korea.

According to his analysis, it is likely the torrent site was hijacking Autonomous System (AS) numbers to hide its true location.

Another analysis on [Hacker News](#) also found The Pirate Bay hijacked some IP addresses, set up a fake Border Gateway Protocol (BGP) advertisement and generated an artificial delay. "They are faking [or] spoofing the ICMP responses. They are also prepending their route advertisement with corresponding AS paths to further disguise it," noted Hacker News.

Topics: [Security](#), [Korea](#), [Networking](#)

## Mögliche Ursachen für Topology-Disorder?

- Angriff?
- Fehlkonfiguration?
- Software-Bug?

## Mögliche Ursachen für Topology-Disorder?

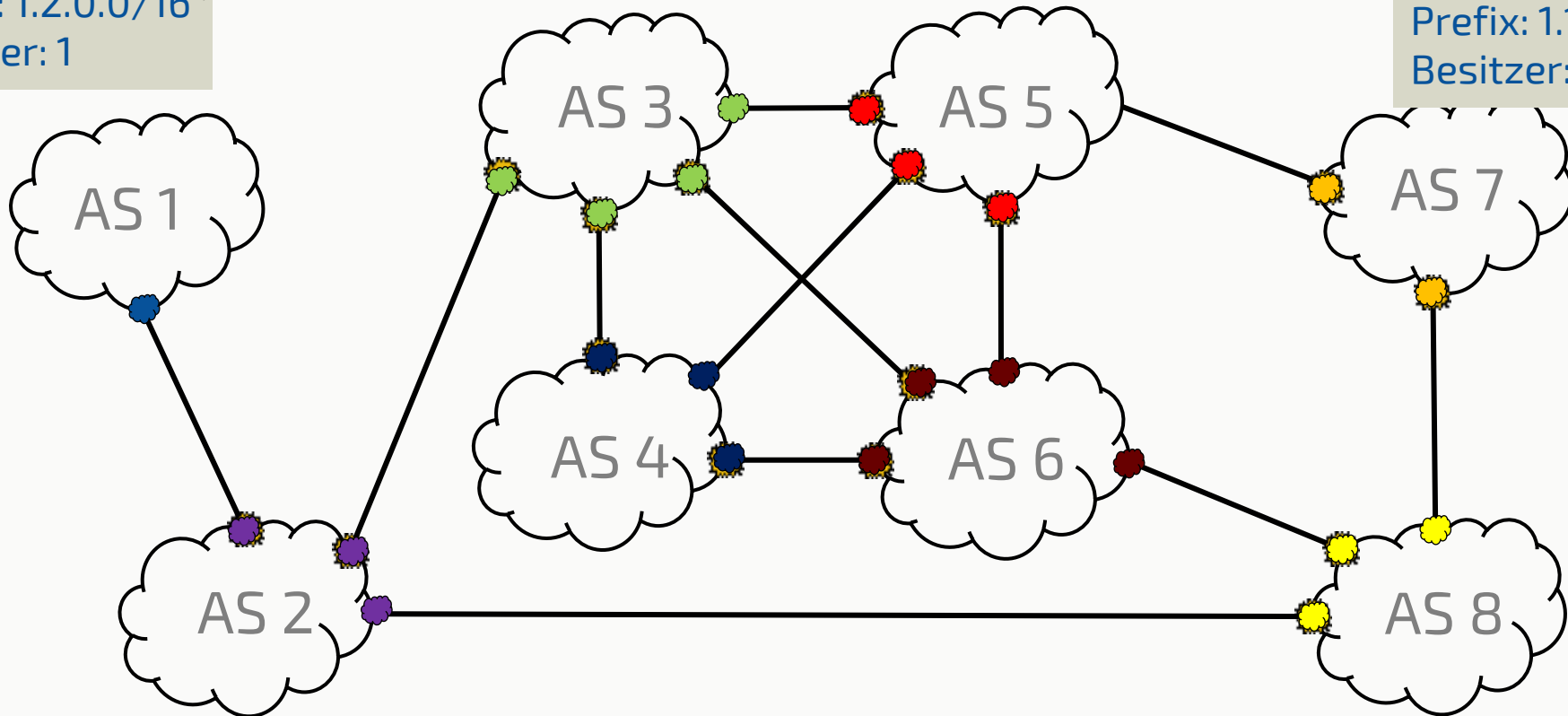
- Angriff?
  - Möglich, und wie gezeigt, sehr effektiv
- Fehlkonfiguration?
  - Pfade werden im Router automatisch erstellt, wenn Announcements weitergeleitet werden. Keine manuelle Tätigkeit im Prozess => eher unwahrscheinlich
- Software-Bug?
  - Generell möglich, aber: Pfadberechnung ist Teil der Testumgebung von Router-Herstellern. Die Verbreitung defekter Software (in diesem Bereich) ist sehr unwahrscheinlich

## Folgen von Topology-Disorder-Angriffen:

- Man-in-the-middle kann Verbindungen mitlesen / manipulieren / verhindern
- Man-on-the-side kann Verbindungen mitlesen
- Wenn die Verbindung richtig kryptografisch abgesichert ist
  - Vertraulichkeit => keine Gefahr
  - Verfügbarkeit => realistische Bedrohung
  - Integrität => keine Gefahr
  - Zurechenbarkeit => keine Gefahr

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological Disorder
  - Angriffsszenario “Quantuminsert”
- Prefix-Hijacking
- Analyse von Routinganomalien

Prefix: 1.2.0.0/16  
Besitzer: 1

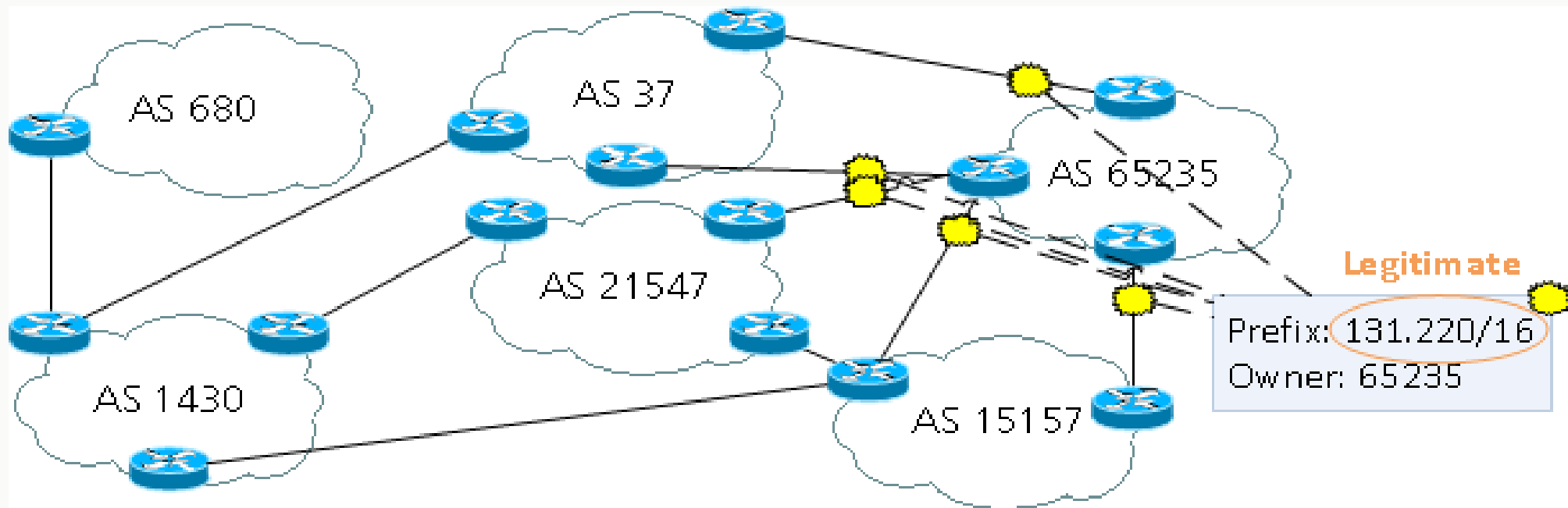


Prefix: 1.1.0.0/16  
Besitzer: 7

# ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

- Ziel: Datenverkehr, der eigentlich für AS 65235 gedacht ist

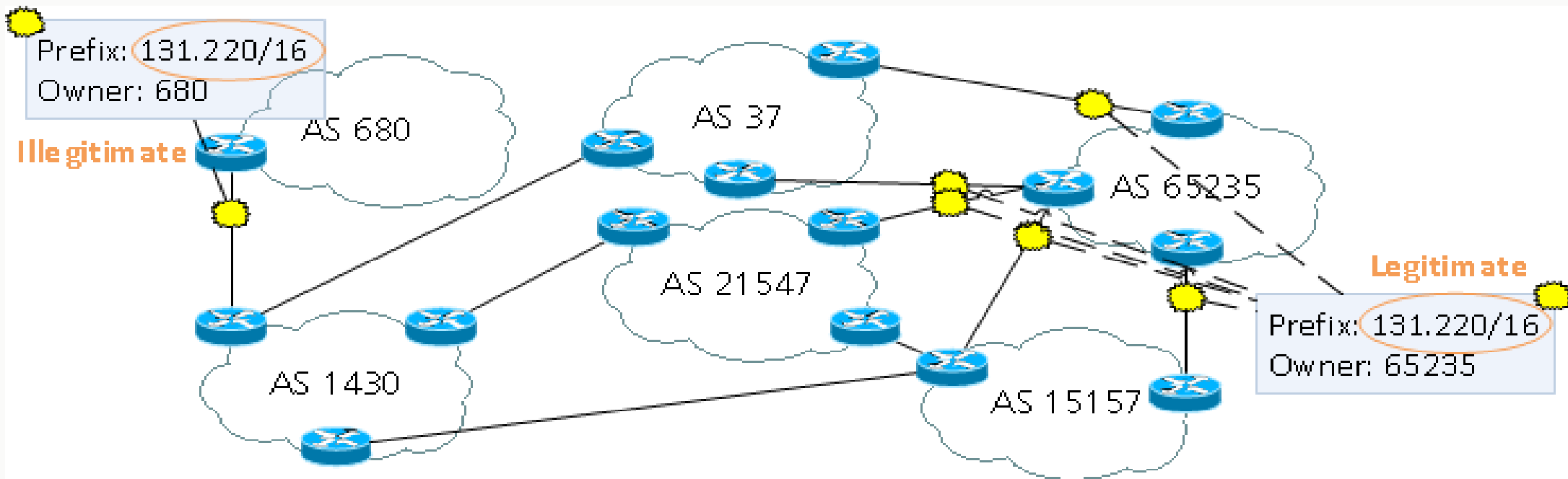




# ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

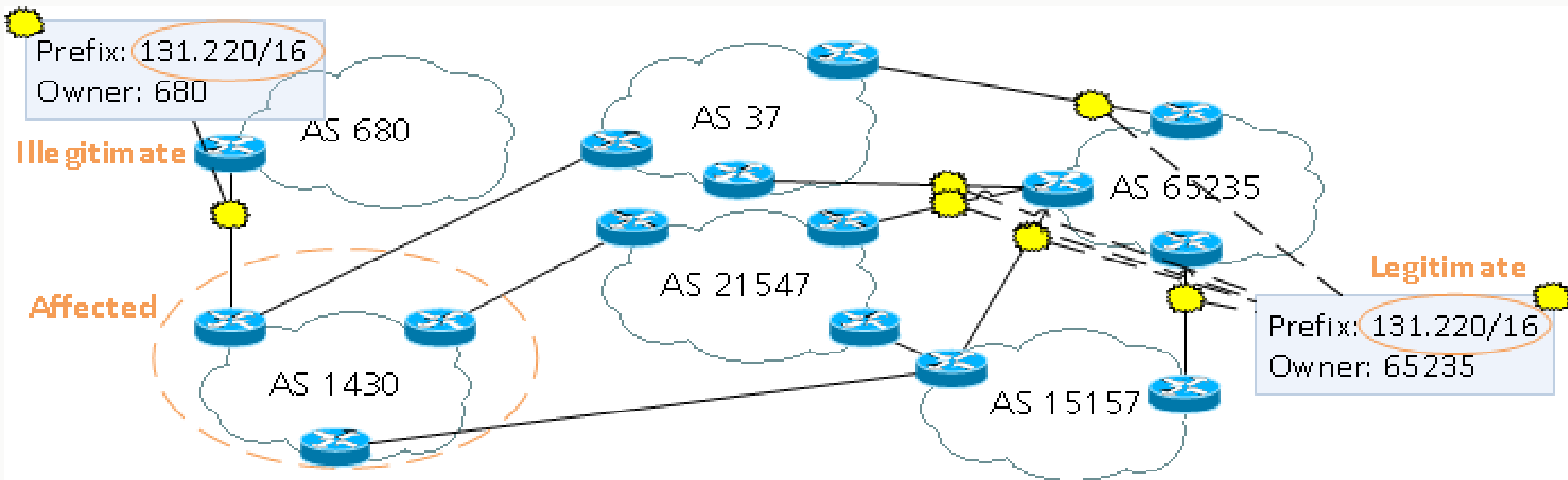
- Was kann passieren?
- Welches AS ist betroffen?



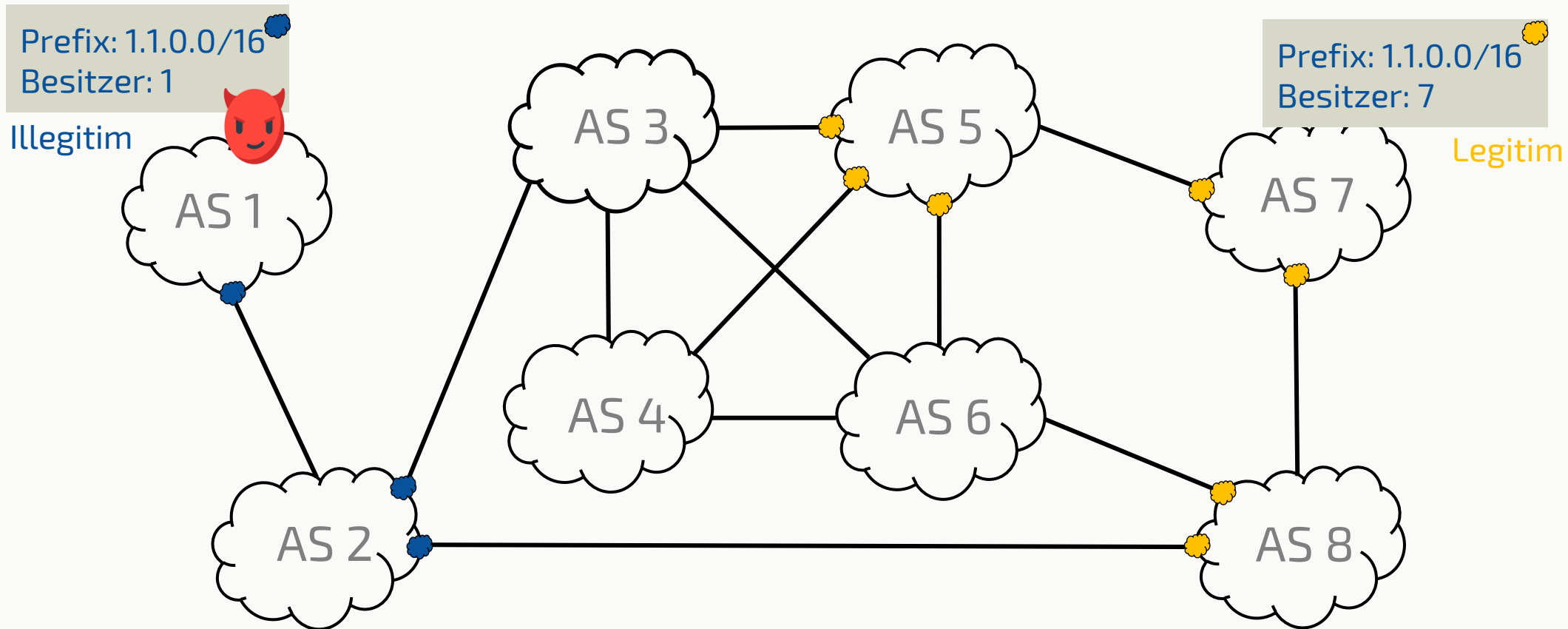
# ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

- Ist dies ein realistisches Szenario (= eine echte Bedrohung)?



# PREFIX-HIJACKING



## *ROUTING ANOMALIES – PREFIX HIJACKING*

- Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)
  - Ist dies ein realistisches Szenario (= eine echte Bedrohung)?



Search CNET



Reviews

News

Video

How To

Games

Download

Log In / Join



US E

CNET > Tech Culture > How Pakistan knocked YouTube offline (and how to make sure it never happens again)

# How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

by Declan McCullagh @declanm / February 25, 2008 2:30 PM PST / Updated: February 25, 2008 4:28 PM PST

3 / f o / o / o / o / 8+ / more +



This graph that network-monitoring firm Keynote Systems provided to us shows the worldwide availability of YouTube.com dropping dramatically from 100 percent to 0 percent for over an hour. It didn't recover completely until two hours had elapsed.

Keynote Systems

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company managed to cut YouTube off the global Web highlights a long-standing security weakness in the way the Internet is managed.

## THIS WEEK'S MUST READS /

- 1 **How Pakistan knocked YouTube offline (and how to make sure it never happens again)**  
Tech Culture
- 2 **Google's Android Wear software will let you leave your phone at home (if there's Wi-Fi)**  
Mobile
- 3 **Twitter makes it easier for strangers to send direct messages**  
Internet
- 4 **This is what a 'Game of Thrones' spring break looks like**  
Tech Culture
- 5 **With Fizz, Google hopes to bring new power to mobile Web**  
Software

## RISK ASSESSMENT / SECURITY &amp; HACKTIVISM

## How China swallowed 15% of 'Net traffic for 18 minutes

In April 2010, 15 percent of all Internet traffic was suddenly diverted ...

by **Nate Anderson** - Nov 17, 2010 8:45pm CET

[Share](#) [Tweet](#) [54](#)

In a [300+ page report](#) (PDF) today, the US-China Economic and Security Review Commission provided the US Congress with a detailed overview of what's been happening in China—including a curious incident in which 15 percent of the world's Internet traffic suddenly passed through Chinese servers on the way to its destination.

Here's how the Commission describes the incident, which took place earlier this year:

For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from US government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

The culprit here was "IP hijacking," a well-known routing problem in a worldwide system based largely on trust. Routers rely on the Border Gateway Protocol (BGP) to puzzle out the best route between two IP addresses; when one party advertises incorrect routing information, routers across the globe can be convinced to send traffic on geographically absurd paths.

This happened famously in 2008, when Pakistan blocked YouTube. The block was meant only for internal use, and it relied on new routing information that would send YouTube requests not to the company's servers but into a "black hole."

As we [described the situation at the time](#), "this routing information escaped from Pakistan Telecom to its ISP PCCW in Hong Kong, which propagated the route to the rest of the world. So any packets for YouTube would end up in Pakistan Telecom's black hole instead." The mistake broke YouTube access from across much of the Internet.

The China situation appears to have a similar cause. The mistaken routing information came from IDC China Telecommunications, and it was then picked up by the huge China Telecom. As other routers around the world accepted the new information, they began funneling huge amounts of US traffic through Chinese servers, for 18 minutes.

As with many things involving cyberattacks and Internet security, it's hard to know if anything bad

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company managed to cut YouTube off the global Web highlights a long-standing security weakness in the way the Internet is managed.

## YouTube offline (and it never happens again)

At addresses were hijacked. But if it spurs interest in

08 4:28 PM PST



is the worldwide  
or over an hour. It

## THIS WEEK'S MUST READS /

1

**How Pakistan knocked YouTube offline (and how to make sure it never happens again)**

Tech Culture

2

**Google's Android Wear software will let you leave your phone at home (if there's Wi-Fi)**

Mobile

3

**Twitter makes it easier for strangers to send direct messages**

Internet

4

**This is what a 'Game of Thrones' spring break looks like**

Tech Culture

5

**With Fizz, Google hopes to bring new power to mobile Web**

Software

## How the Internet in Australia went down under

Posted by Andree Toonk - February 27, 2012 - [BCP instability](#) - 2 Comments

This Wednesday for about 30 minutes many Australians found themselves without Internet access. All these users were relying either directly or indirectly on the Telstra network, which at that point was isolated from the Internet. This story quickly hit [the local headlines](#), in this blog we'll look at the technical details of this event and what the cause of this outage likely was.

Telstra is one of Australia's major Internet providers. It normally originates approximately 500 IPv4 prefixes and 3 IPv6 prefixes. Telstra also provides Transit for many ISPs and enterprises such as for example AS38285 'Dodo' an Australian ISP and AS10235 'National Australia Bank'. So how could such a large provider go down, surely it has lots of redundant hardware and multiple connections in and out of the country?

As it turns out Wednesday's outage was caused by a routing error many network engineers have first hand experience with, a simple routing leak. A routing leak can happen when small ISP X buys transit from ISP A and also from ISP B. ISP X receives a full BGP routing table from A and because of incorrect filtering relays these messages to ISP B. As a result ISP B now learns all Internet routes via ISP X to ISP B and ISP X (the customers) now became an upstream provider for ISP B.

The above is likely what happened last Wednesday between Telstra and Dodo (AS38285). Dodo a Telstra customer, re-announced all Internet routes to Telstra, which because it prefers customer routes now thinks the best way to the Internet is through Dodo. [This post](#) on the Ausnig mailings list shows how Telstra was using Dodo (a customer) as transit to reach a network in India.

This is not a new zero day attack scenario or anything like it. Instead it's probably the number one mistake when configuring BGP routing. I remember when I was just learning about BGP my mentor always used to tell me.. Filter, Filter, Filter, filter!! Which is exactly what didn't happen here. Because it is so easy to accidentally leak routes in BGP you have to explicitly define filters that prevent this. In this case Dodo should have had filters to make sure they would only announce their prefixes and Telstra should have had these filters as well to prevent hijacks but more importantly to protect its own infrastructure. In this case these filters did not seem to be in place, which allowed this leak to happen.

However, this alone should not have brought down all of Telstra's International connections. So what happened? It's likely that Telstra now tagged all routes learned from Dodo (all 400,000 of them) as customer routes and faithfully announced this to all of its peers and upstream providers.

As keeping large filters up to date can be tedious we often see large providers use a mechanism known as max prefix limits. Instead of explicitly defining which prefixes to allow the number of prefixes expected plus some extra is set as the maximum number of prefixes allowed. This is useful to prevent a sudden spike in announcements, often caused by leaks. In case the limit is reached the BGP session is brought down to prevent the leak from spreading.

Connect with us

Download

Log In / Join

US E

NG

## ie (and ain)

t spurs interest in

EADS /

**Pakistan knocked YouTube**  
**s (and how to make sure it never**  
**ens again)**

Culture

**le's Android Wear software will**  
**u leave your phone at home (if**  
**'s Wi-Fi)**

**r makes it easier for strangers**  
**id direct messages**

st

**s what a 'Game of Thrones'**  
**g break looks like**

Culture

**'Fizz, Google hopes to bring new**  
**r to mobile Web**

ire

023

47

ars te

MAIN MENU

RISK ASS

## How Chi

18 min

In April 2010, 15

by **Nate Anderson** - No  
In a **300+ page rep**  
provided the US Cc  
curious incident in  
servers on the way

Here's how the Cor

For about 18 m  
routes that instr  
Other servers a  
percent of the li  
traffic to and fr  
Senate, the arr  
the National A  
Oceanic and At  
also affected, si

The culprit here wa  
on trust. Routers re  
IP addresses; wher  
be convinced to se

This happened fair  
internal use, and it  
company's servers

As we **described th**  
its ISP PCCW in Hc  
YouTube would en  
from across much i

The China situatio  
China Telecommun  
around the world a  
through Chinese si

As with many thing:  
**Angieprom**  
managed to  
Internet is n

22. Mai 2028



## How China's Internet Censorship

In April 2010, 151

by Nate Anderson - No

In a 300+ page report provided the US Congress, a curious incident in the servers on the way

Here's how the Cor

For about 18 minutes routes that instruct Other servers a percent of the Internet traffic to and from the Senate, the arm the National Aeronautics and Space Administration also affected, si

The culprit here was on trust. Routers re IP addresses; when be convinced to se

This happened far internal use, and it company's servers

As we described th its ISP PCCW in Hong YouTube would en from across much o

The China situation China Telecommun around the world a through Chinese si

As with many thing:

Angieproton

managed to

Internet is n

## How the Internet in Australia

Posted by Andree Toonk - February 27, 2012 - BCP ins

This Wednesday for about 30 minutes many All these users were relying either directly or was isolated from the Internet. This story qu technical details of this event and what the

Telstra is one of Australia's major Internet p prefixes and 3 IPv6 prefixes. Telstra also pr for example AS38285 'Dodo' an Australian such a large provider go down, surely it has and out of the country?

As it turns out Wednesday's outage was ca first hand experience with, a simple routing transit from ISP A and also from ISP B. ISP X r incorrect filtering relays these messages to ISP X to ISP B and ISP X (the customers) now

The above is likely what happened last We Telstra customer, re-announced all Internet routes now thinks the best way to the Intern list shows how Telstra was using Dodo (a c

This is not a new zero day attack scenario mistake when configuring BGP routing. I rem always used to tell me.. Filter, Filter, Filter, fil Because it is so easy to accidentally leak ro prevent this. In this case Dodo should have prefixes and Telstra should have had these protect its own infrastructure. In this case th this leak to happen.

However, this alone should not have broug what happened? It's likely that Telstra now them) as customer routes and faithfully ann

As keeping large filters up to date can be te known as max prefix limits. Instead of explic prefixes expected plus some extra is set as to prevent a sudden spike in announcement BGP session is brought down to prevent the

ABOHAMEHT  
SUBSCRIBE

Home

Archive

Search

Sponsors

About us

Contact

Donation



CURRENT ISSUE



Оръжията на  
Русия



Лобиране в  
Брюксел



Хрониките на  
Тейтъм



НАТО - мит и  
фикция

## Hijacked? UK's Nuclear Weapons Data Re-Routes and Travels via Ukraine



**Sensitive internet data from British company Royal Mail and the UK Atomic Weapons Establishment (AWE) has passed through Russia and Ukraine via insecure connections, according to internet performance and analysis company Dyn.**

An article published in technewstoday.com, suggests "web traffic originating from Texas, intended for certain addresses in the UK has been taking an unconventional route to its destination, through Ukraine and Russia".

According to research carried out by Dyn, Ukrainian telecom provider Vega "began announcing 14 British Telecom (BT) routes, resulting in the redirection of Internet traffic through Ukraine for a handful of BT customers". This includes the UK's Atomic Weapons Establishment.

AWE is 'responsible for the design, manufacture and support of warheads for the United Kingdom's nuclear deterrent'.



# HACKER REDIRECTS TRAFFIC FROM 19 INTERNET PROVIDERS TO STEAL BITCOINS



Adam Voorhes Gail Anderson + Joe Newton

1K



AMONG ALL THE scams and thievery in the bitcoin economy, one recent hack sets a new bar for brazenness: Stealing an entire chunk of raw internet traffic from more than a dozen internet service

# СТРОГО СЕКРЕТНО

СТРОГО СЕКРЕТНО

Krassimir Ivandjiski

CURRENT ISSUE



Оръжията на Русия



Лобиране в Брюксел



Хрониките на Тейтъм



НАТО - мит и фикция

Nuclear Weapons Data Re-Routes and ine



om British company Royal Mail and the UK Atomic Weapons s passed through Russia and Ukraine via insecure connections, formance and analysis company Dyn.

anewstoday.com, suggests "web traffic originating from Texas, issues in the UK has been taking an unconventional route to its ine and Russia".

ied out by Dyn, Ukrainian telecom provider Vega "began announcing ites, resulting in the redirection of Internet traffic through Ukraine ers". This includes the UK's Atomic Weapons Establishment.

а design, manufacture and support of warheads for the United nt'.

# HACKER FROM 19 TO STEA



Adam Voorhes Gail

1K



AMON  
econo  
braze  
traffic

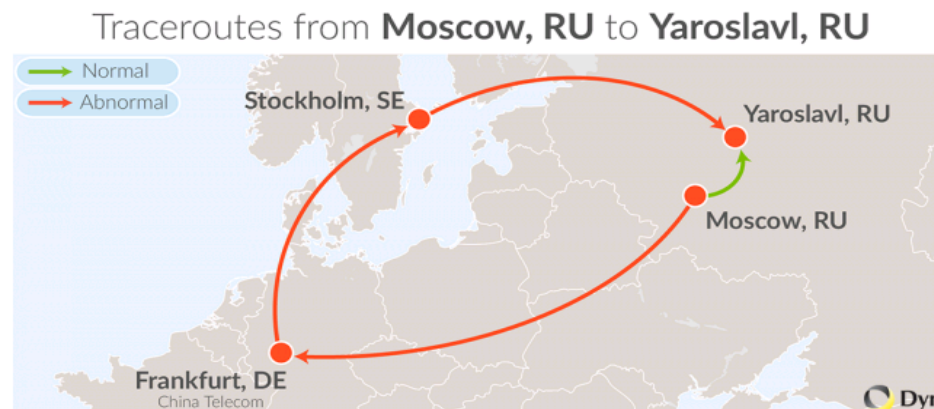
## RISK ASSESSMENT / SECURITY & HACKTIVISM

### WTF, Russia's domestic Internet traffic mysteriously passes through Chinese routers

Unexplained diversion underscores insecurity of Net's global routing system.

by Dan Goodin - Nov 9, 2014 7:00pm CET

Share Tweet 74



Enlarge

Dyn Research

Domestic Internet traffic traveling inside the borders of Russia has repeatedly been rerouted outside of the country under an unexplained series of events that degrades performance and could compromise the security of Russian communications.

The finding, reported Thursday in a [blog post published by Internet monitoring service Dyn](#), underscores the fragility of the border gateway protocol (BGP), which forms the underpinning of the Internet's global routing system. In this case, domestic Russian traffic was repeatedly routed to routers operated by China Telecom, a firm with close ties to that country's government. When huge amounts of traffic are diverted to far-away regions before ultimately reaching their final destination, it increases the chances hackers with the ability to monitor the connections have monitored or even altered some of the communications. A similar concern emerged last year, when Dyn found big chunks of traffic belonging to US banks, government agencies, and network

#### FURTHER READING



**REPEATED ATTACKS HIJACK HUGE CHUNKS OF INTERNET TRAFFIC, RESEARCHERS WARN**

Man-in-the-middle attacks divert data on scale never before seen in the wild.

Data Re-Routes and



ail and the UK Atomic Weapons  
Ukraine via insecure connections,  
any Dyn.

web traffic originating from Texas,  
g an unconventional route to its

com provider Vega "began announcing  
in of Internet traffic through Ukraine  
omic Weapons Establishment.

support of warheads for the United

Krassimir  
Ivandjiski

#### CURRENT ISSUE



Оръжията на  
Русия



Лобиране в  
Брюксел



Хрониките на  
Тейтъм



НАТО - мит и  
фигция





Kevin Beaumont

Follow

InfoSec, from the trenches of reality. Email [kevin.beaumont@gmail.com](mailto:kevin.beaumont@gmail.com) | Twitter: [@gossithedog](https://twitter.com/gossithedog) on Twitter.

Apr 24 · 3 min read

## Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed

Between 11am until 1pm UTC today, DNS traffic—the phone book of the internet, routing you to your favourite websites—was hijacked by an unknown actor.



The attackers used BGP—a key protocol used for routing internet traffic around the world—to reroute traffic to Amazon's Route 53 service, the largest commercial cloud provider who count major websites such as Twitter.com as customers.

They re-routed DNS traffic using a man in the middle attack using a server at Equinix in Chicago.

From there, they served traffic for over two hours.

### CURRENT ISSUE



Оръжията на Русия



Лобиране в Брюксел



Хрониките на Тейтъм



НАТО - мит и фикция

## Mögliche Ursachen für Prefix-Hijacking?

- Angriff?
- Fehlkonfiguration?
- Software-Bug?

## Mögliche Ursachen für Prefix-Hijacking?

- Angriff?
  - Ja!
  
- Fehlkonfiguration?
  - Das kann tatsächlich passieren (etwa verursacht durch übermüdete Administratoren an einem Freitagnachmittag) und scheint ein sehr häufiges Phänomen/Problem zu sein
  
- Software failure?
  - Möglich, aber wie Topology Disorder sehr unwahrscheinlich

## *ROUTING ANOMALIES – PREFIX HIJACKING*

- Folgen von Prefix-Hijacking:
  - Nachahmung / Immitation von Kommunikationspartnern / Online-Diensten
  - Traffic Blackholing (= eine Art von Denial-of-Service)
  - Man-in-the-Middle (schwierig, aber theoretisch möglich)

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological-Disorder
  - Angriffsszenario “Quantuminsert”
- Prefix-Hijacking
- Analyse von Routinganomalien

Wie können Topology-Disorder und Prefix-Hijacking erkannt werden?

- Möglichkeiten zur Erkennung von Topology-Disorder:
  - Basierend auf einer vollständigen Karte des Internets (mit allen Peering-Verbindungen zwischen den AS)
  - Überprüfe jeden Pfad aller Announcements
    - Problem: eine solche Karte existiert nicht!
  - Basierend auf einer Routing-Historie (und der AS-Verbindungen)
  - Eine neu erscheinende AS-Verbindung kann bereits bekannt sein (und lediglich für einen gewissen Zeitraum nicht genutzt)
  - Was passiert beim ersten Auftauchen einer AS-Verbindung
    - Problem: Diese Methode kann die Zuverlässigkeit von AS-Verbindungen zeigen, eignet sich aber nicht zur Anomalieerkennung



Wie können Topology-Disorder und Prefix-Hijacking erkannt werden:

- Möglichkeiten zur Erkennung von Topology-Disorder
  - Basierend auf Routing-Historie, verbunden mit zusätzlichen Quellen über AS-Verbindungen (z.B. IXP oder LG) Daten.
  - Nutzung der Wahrscheinlichkeit für die Erstellung einer Verbindung von AS auf Basis bereits bekannter Verbindungen der AS
    - Gibt zusätzliche Hinweise, aber nur für eine überschaubare Anzahl an AS-Verbindungen

Zusätzliche Informationen von IXPs (Internet eXchange Points)

# ROUTING ANOMALIES – ROUTING ANOMALY DETECTION

ACTIVE ASNs ⓘ	CONNECTING ASNs ⓘ	IPv4 ROUTES ⓘ	IPv6 ROUTES ⓘ	LOOKING GLASS →
1071	9	650,150	97,451	

ASN	NAME	MACRO	PEERING POLICY	STATUS ↓
Search for...				
6057	ANTEL URUGUAY	AS-ANTEL-ALL	Open	CONNECTING
<u>8309</u>	SIPARTECH Sarl	AS-SPH	Open	CONNECTING
<u>25058</u>	CMO Internet Dienstleistungen GmbH	AS-CMO	<u>Open</u>	CONNECTING
29469	Global technology of Ukraine			CONNECTING
40630	GridFury, LLC		Open	CONNECTING
205356	SAP SE			CONNECTING
213281	Greenfiber Netz & Management GmbH		Open	CONNECTING
263903	Inforbarra	AS263903:AS- INFORBARRA	Open	CONNECTING
<u>397163</u>	LAX Online Limited Company	AS-LOL-34	<u>Selective</u>	CONNECTING
<u>42</u>	Packet Clearing House	AS-PCH	<u>Open</u>	ACTIVE

<https://www.de-cix.net/en/locations/frankfurt/connected-networks>

## Zusätzliche Informationen von LGs (Looking Glass)



## Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at [route-server.he.net](https://route-server.he.net).

[Show options](#)

core1.ams1.he.net> show ip bgp summary								
Local AS Number			6939					
Number of Neighbors Configured			842, 776 up					
Number of Routes Installed			2942857 (253085702 bytes)					
Number of Routes Advertised			65124013 (5061468 entries) (242950464 bytes)					
Number of Attribute Entries			526348 (47371320 bytes)					
Neighbor Address	ASN	State	Time	Rt:Accepted	Rt:Filtered	Rt:Sent	Rt:ToSend	
72.14.212.34	15169	ESTAB	173d 8h25m	342	0	23778	0	
80.249.208.1	1200	ESTAB	147d 2h15m	3	1	66404	0	
80.249.208.26	26496	ESTAB	12d10h 0m	493	0	66404	0	
80.249.208.27	29075	ESTAB	173d 8h25m	226	0	66404	0	
80.249.208.29	8304	ESTAB	4d 1h42m	27	0	66404	0	
80.249.208.30	8529	ESTAB	50d 9h14m	4308	33	66404	0	
80.249.208.31	16637	ESTAB	40d 9h19m	505	0	66404	0	
80.249.208.32	12871	ESTAB	25d 9h57m	14	0	66404	0	
80.249.208.33	559	IDLE	1h 9m25s	0	0	0	66404	
80.249.208.34	1103	ESTAB	73d16h19m	189	5	66404	0	
80.249.208.35	12859	ESTAB	47d18h16m	70	0	66404	0	
80.249.208.37	2686	ESTAB	32d 7h33m	356	0	66404	0	
80.249.208.38	4589	ESTAB	33d 9h57m	251	0	66404	0	
80.249.208.39	112	ESTAB	3d22h 1m	1	0	66404	0	
80.249.208.42	9145	ESTAB	41d 9h16m	219	0	66404	0	
80.249.208.43	2611	ESTAB	50d 8h48m	55	0	66404	0	
80.249.208.45	43855	ESTAB	73d16h19m	0	0	66404	0	

<https://lg.he.net/>

## Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:

- Definition:

Let prefix  $p$  being associated with two paths

$asp_1 = (p_1, p_2, \dots, p_n)$  and

$asp_2 = (q_1, q_2, \dots, q_m)$

then, a MOAS conflict occurs if  $p_n \neq q_m$ .

- Drei Klassen von MOAS-Konflikten:

OrigTransAS:  $p_n = q_j (j < m)$

SplitView:  $p_i = q_j (i < n, j < m)$

DistinctPaths:  $p_i \neq q_j (\forall i \in [1..n], j \in [1..m])$

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Im Bezug auf Prefixe könnte eine vierte Klasse “Sub-MOAS” definiert werden:

Let prefix  $p$  and prefix  $q$  be related in a form that  $q < p$  (i.e.  $q$  is a real subnet of  $p$ ) and a MOAS conflict occurs for all IP addresses in  $q \cap p$ .

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Basierend auf annoncierten Prefixen
  - Teste für alle Announcements desselben Prefixes, ob es ein MOAS ist
- Wo gibt es annoncierte Prefixe?



Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Basierend auf annoncierten Prefixen
  - Teste für alle Announcements desselben Prefixes, ob es ein MOAS ist
- Wo gibt es annoncierte Prefixe?
  - RIPE RIS, RouteViews, PCH, ... sammeln und archivieren BGP-Announcements

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Wo gibt es annoncierte Prefixe?
  - RIPE RIS
    - Standorte: Amsterdam, London, Paris, Geneva, Vienna, Otemachi (Japan), Stockholm, San Jose, Zurich, Milan, New York, Frankfurt, Moscow, Palo Alto, Sao Paulo
    - <https://www.ripe.net/data-tools/stats/ris/>
  - RouteViews
    - Oregon, Ashburn, Palo Alto, Nairobi (Kenya), London, Portland, Tokyo, Sydney, Sao Paulo, Atlanta, Fort Collins
    - <https://www.routeviews.org/>
  - PCH
    - Mehr als 50 Standorte.
    - <https://www.pch.net/resources/data.php>

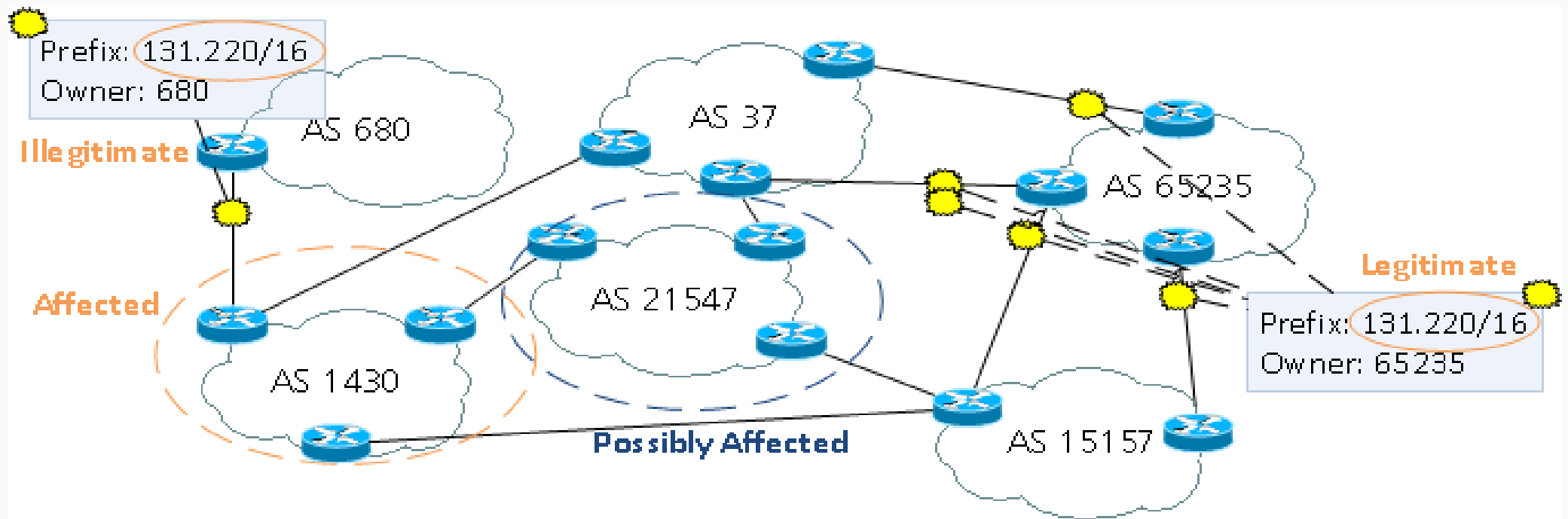
## *ROUTINGANOMALIEN – PREFIX-HIJACKING*

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

# ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



## ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$V$	: the set of all ASs (vertices)
$A = V \setminus \{t\}$	: the set of all possible attackers for a given true origin $t \in V$ .
$N = V \setminus \{t, a\}$	: the remainder of $V$ for chosen origin $t \in V$ and attacker $a \in A$
$P_{(t,a,n)}$	: the set of connected ASs providing shortest paths to the origins $t \in V$ or $a \in A$ to $n \in N$

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$\beta(t, a, n) = \begin{cases} 0 & , \text{ if Case 1} \\ \frac{1}{|P_{(t,a,n)}|} & , \text{ if Case 2} \\ \sum_{p \in P_{(t,a,n)}} \frac{1}{|P_{(t,a,n)}|} \times \beta(t, a, p) & , \text{ if Case 3} \end{cases}$$

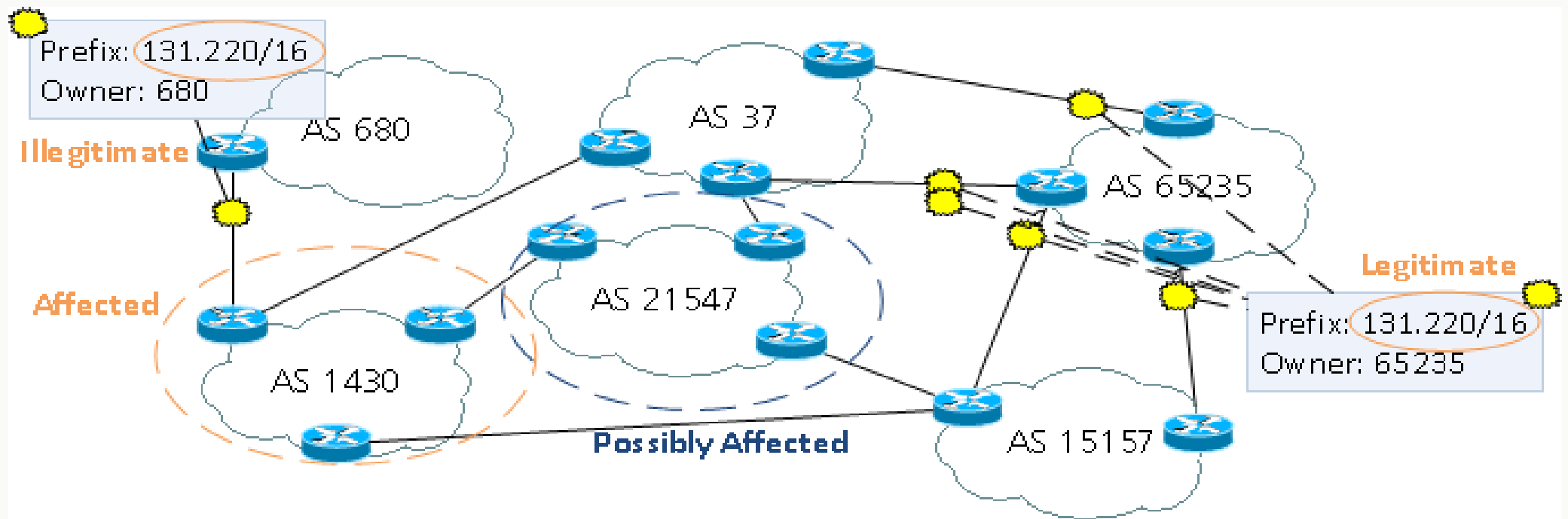
*Case 1:*  $t$  is not, but  $a$  is directly connected to  $n$ .

*Case 2:*  $t$  is and  $a$  might be directly connected to  $n$ .

*Case 3:* both,  $t$  and  $a$  are not directly connected to  $n$ .

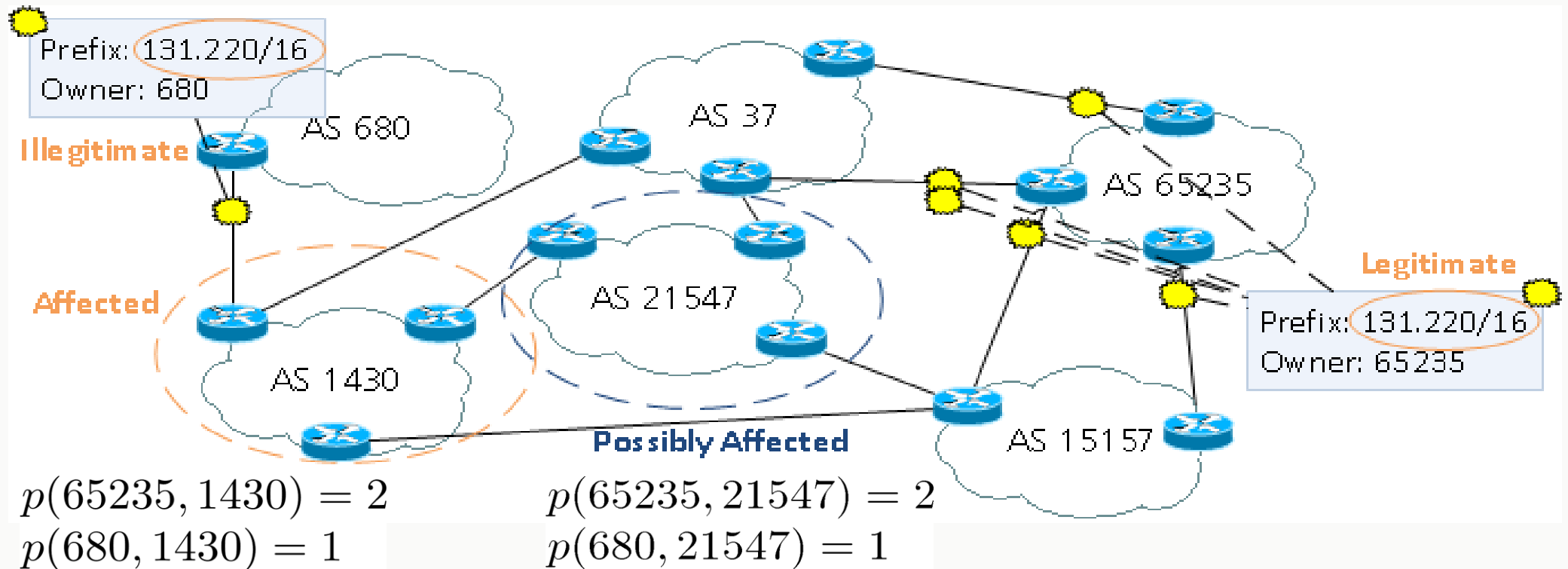
# ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



# ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

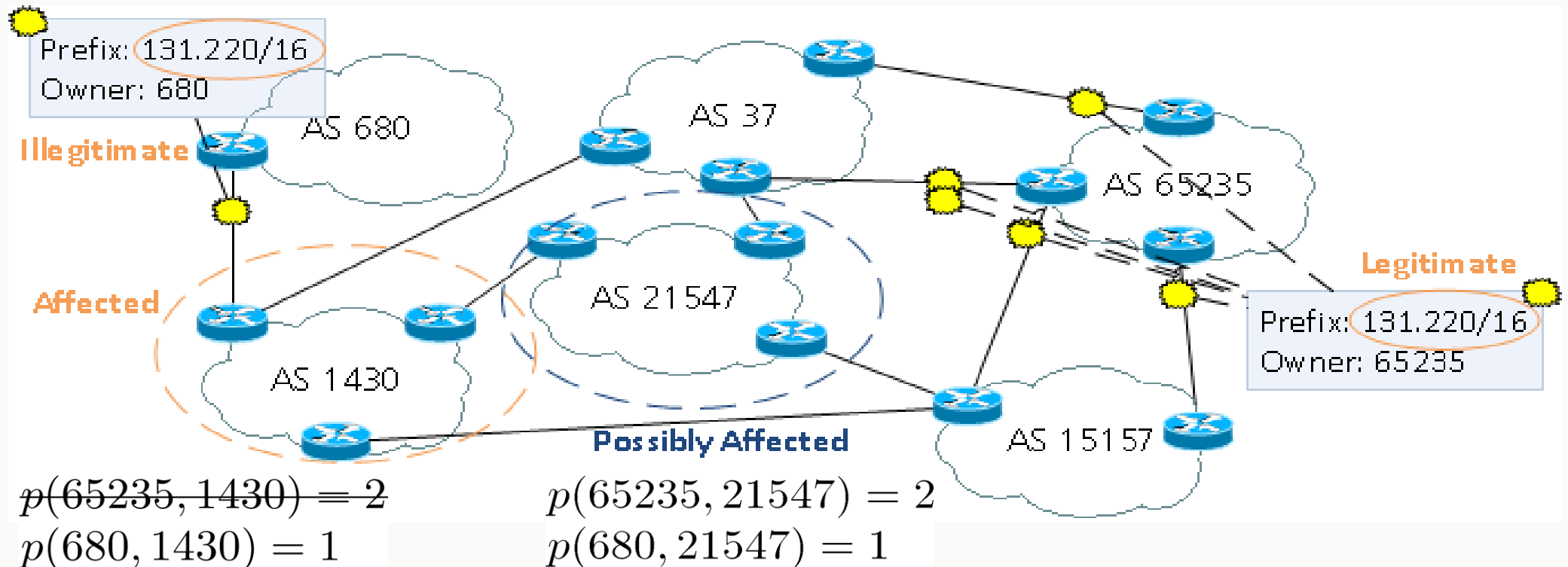


- $p(t,n)$ : Anzahl der kürzesten Pfade von t nach n (bezogen nur auf die Pfade von t -> n)



# ROUTINGANOMALIEN – PREFIX HIJACKING

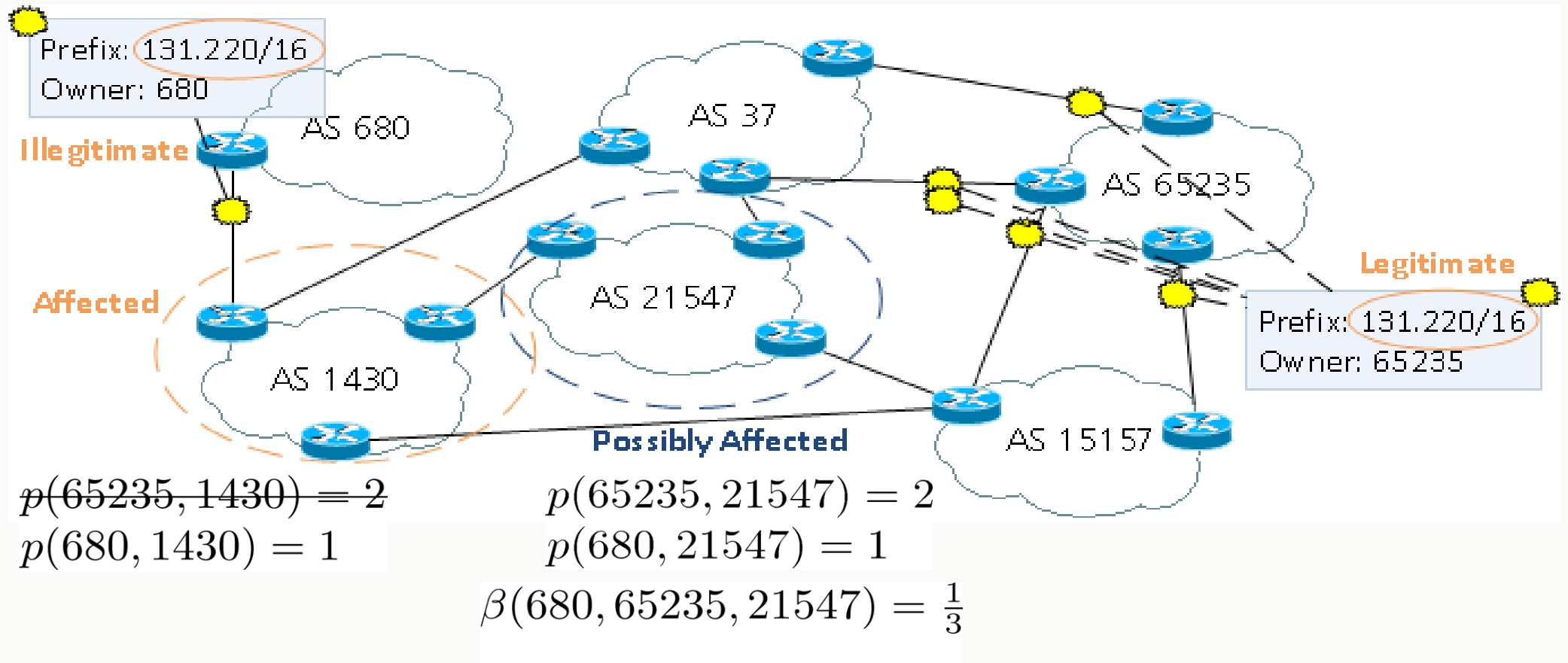
Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



Not in tie-break!

# ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



## *ROUTINGANOMALIEN – PREFIX HIJACKING*

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$\beta(680, 65235, 21547) = \frac{1}{3}$$

- Das ist lediglich der Einfluss von AS 680 bezogen auf AS 21547 für Prefixe, die auch von AS 65235 annonciert werden
- Wie lässt sich der Einfluss (Impact) generalisieren?

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$\beta(680, 65235, 21547) = \frac{1}{3}$$

- Das ist lediglich der Einfluss von AS 680 bezogen auf AS 21547 für Prefixe, die auch von AS 65235 annonciert werden
- Wie lässt sich der Einfluss (Impact) generalisieren?

$$I(a) = \sum_{t \in V \setminus \{a\}} \sum_{v \in N} \frac{\beta(a, t, v)}{|V \setminus \{a\}| |N|}$$

- Äußere Summe über  $|V| - 1$  (True Origins - ohne den Angreifer).
- Innere Summe über  $|V| - 2$  ASes (ohne den Angreifer und ohne True Origin)

## ***ROUTINGANOMALIEN – PREFIX HIJACKING***

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wie widerstandsfähig ist ein AS (zur Verteidigung des eigenen Prefixes)?

## *ROUTINGANOMALIEN – PREFIX HIJACKING*

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wie widerstandsfähig ist ein AS (zur Verteidigung des eigenen Prefixes)?
- Widerstandsfähigkeit (Resilience)

$$R(t) = \sum_{a \in A} \sum_{v \in N} \frac{\beta(t, a, v)}{|A||N|}$$

- Offensichtlich: Die Resilience eines AS ist gleich dem Impact, den das AS als Angreifer hätte, wenn die Rollen vertauscht wären.

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 5. Juni 2023

Nächste Übung:

- Dienstag, 23. Mai 2023 – 16 Uhr
- Abgabe des Übungszettels bis morgen – 16 Uhr