It's all trash or not?

The Network Blackhole: An Independent Lens on Regulatory Claims

Gérard WAGENER – CIRCL

Cynthia WAGNER – Fondation Restena

NISDUC Conference Luxembourg
07th May 2025

Introduction

Networks are busy places

Referring to a statistic institute* a forecast for 2025 claims:

- 48-75 billions connected devices → 8 billion people
- up to 46Zbytes of data

Besides legitimate traffic there is

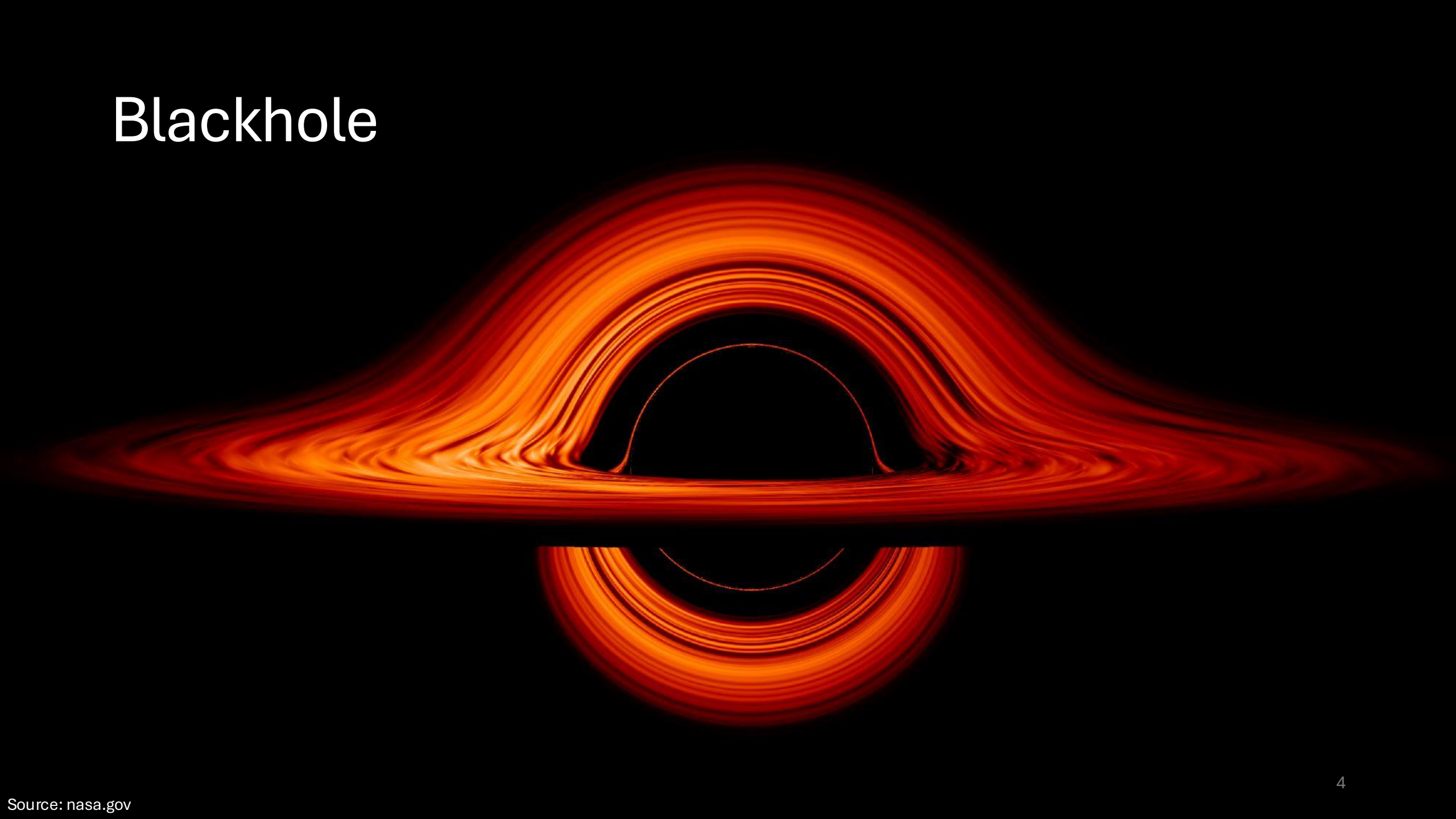
- traffic for attacks
- Unwanted traffic
  - erroneous traffic
  - scanning activities
  - …

*: www.statista.com

It’s all trash…or not?

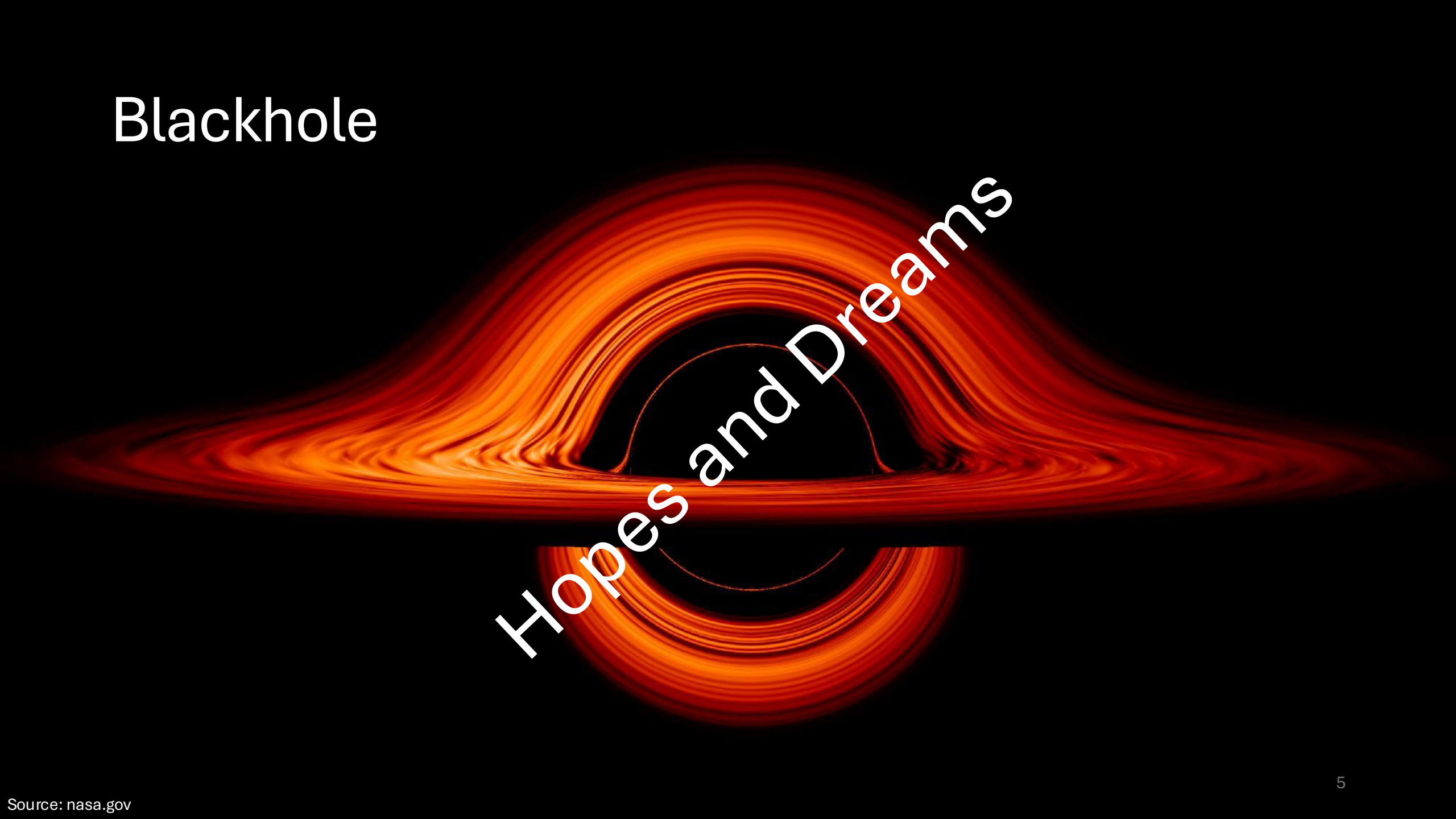
Speaking about unwanted traffic, are all those packets simply trash?

Blackhole



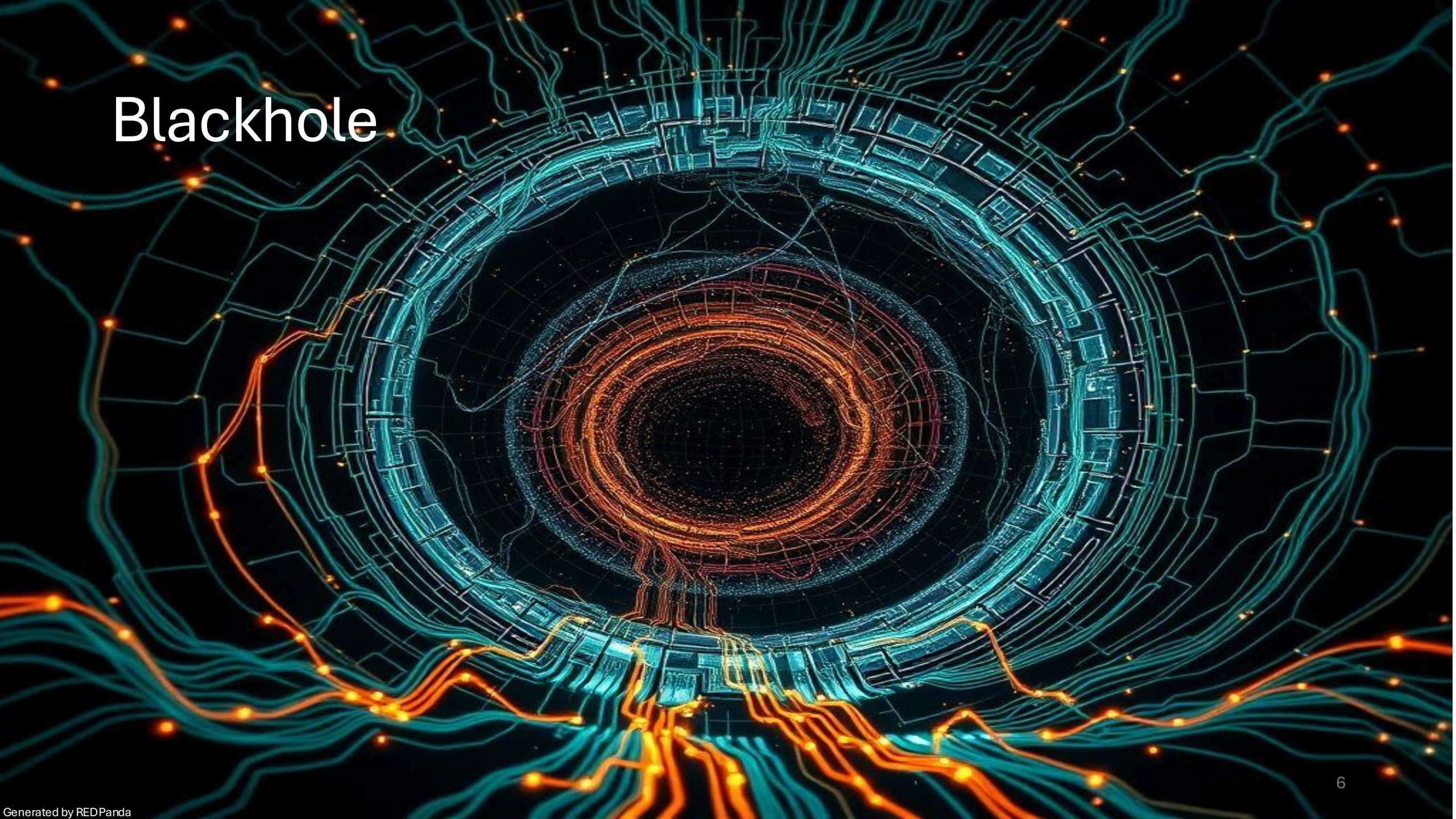
Source: nasa.gov

Blackhole



Source: nasa.gov

Blackhole



Blackhole

- The Blackhole sensor is currently on unused IP address space
- Traffic to the blackhole is Unidirectional
- Captures unwanted traffic
- Fun part - the blackhole is located on a IP address range that is resembles to private address space

What ends in the Blackhole?

- Scanning activities
- Backscatter from Distributed denial of service attacks
- Mass exploitation of devices
- Misconfigured devices
- Unexpected activities
- …Many more

The Why about data in the blackhole

Scanning and mass exploitation

Spelling mistakes leading to erroneous configs and connections

Default routing is configured

Outgoing connections are poorly filtered

Due to complex redundancy setups, the impact of erroneous configurations often goes unnoticed

Who do we see in the blackhole

Electricity, heating & cooling data → Energy sector

Railway protocol data → transport sector

Cryptocurrency data → Finance sector

Medical device data → Health sector

Core Internet protocols, DNS resolver, cloud, telecom data → Digital Infrastructure and ICT service management sector

→ Many of the NIS2 sectors

→ **Due to convergence to Ethernet / IP protocols / tunneling**

What we see in the blackhole (**cont**)

- Limitations of Packet Captures
- Only IP packets are recorded in the captures
- Traffic is unidirectional
- Traffic may be forged or spoofed
- Difficult to distinguish between:
  - Scanning activity
  - Mass exploitation attempts
  - Misconfigured devices

Using the data

- Traffic filtering approach
  - Source IPs that probe more than one target IP in the blackhole network within one hour are considered scanning or mass exploitation sources.
  - Packets with erroneous formats were discarded.
  - Sources that appear repeatedly are classified as misconfigured devices.

Dataset description for this presentation

Collection start date:
2025-01-01

Collection end date:
2025-04-14

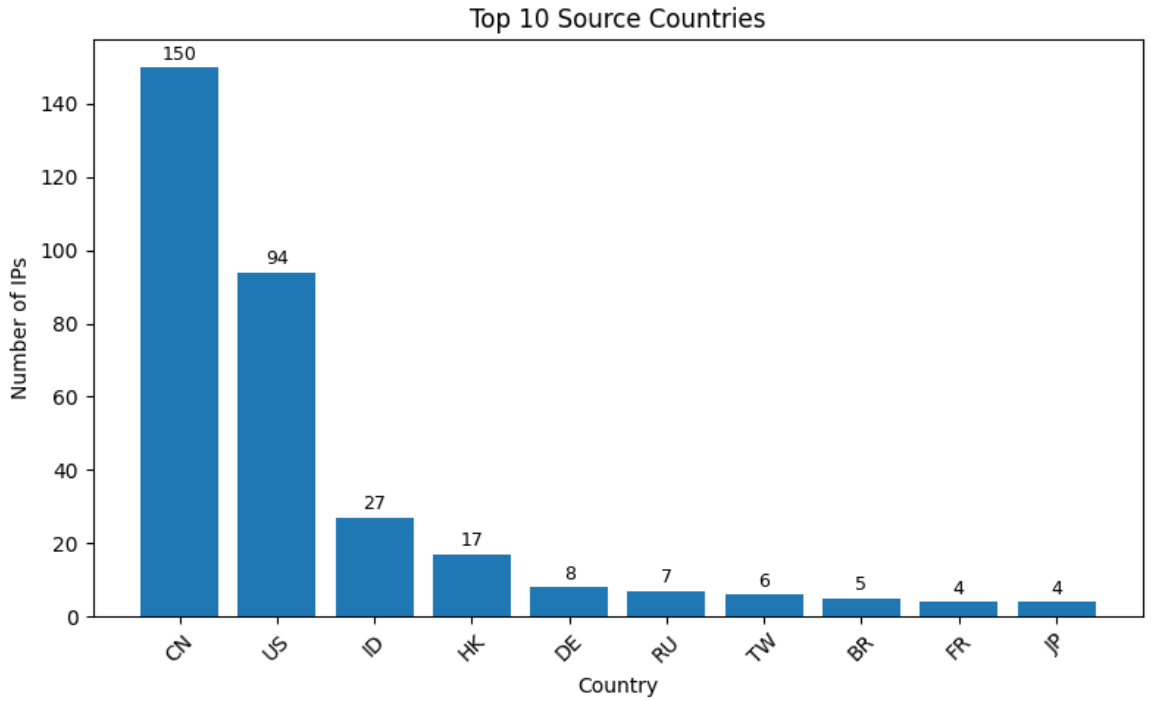
Volume: 632 GB

CNIP Protocol Example

- CN/IP is defined in standard EIA/CEA-852
- Used to transport component network frames such as LON over UDP or TCP
- Applied in Building control systems for lighting and HVAC (intelligent buildings) and Smart meters
- LonTalk is used in
  - industry automation,
  - railway stations,
  - on-train telemetry,
  - many more.

CNIP Protocol Example

Total Events: 10713



Infiniband Example

- Often used by Network Video Transmitters
- https://www.dahuasecurity.com/asset/upload/uploads/soft/20200805/DH-IPC-HFW5221E-Z_Datasheet_20200805
- Features:
  - Face Detection
  - Face Attributes
  - Perimeter Protection

    People Counting

Infiniband Example

- Identified device probing blackhole:
- DH-IPC-HFW5221E-Z

```
<a:Address>uuid:a004713c-1852-4b16-939e-b99e46d67852</a:Address>
    </a:EndpointReference>
    <d:Types>dn:NetworkVideoTransmitter tds:Device</d:Types>
    <d:Scopes>
     onvif://www.onvif.org/location/country/china
     onvif://www.onvif.org/name/Dahua
     onvif://www.onvif.org/hardware/IPC-HFW5221D-Z
     onvif://www.onvif.org/Profile/Streaming
     onvif://www.onvif.org/type/Network_Video_Transmitter
     onvif://www.onvif.org/extension/unique_identifier
     onvif://www.onvif.org/Profile/Q/Operational
    </d:Scopes>
    <d:XAddrs>http://192.168.202.128/onvif/device_service</d:XAddrs>
```

Infiniband Example

- Identified device probing blackhole:
- DH-IPC-HFW5221E-Z

2025-04-01: 62 packets
2025-04-02: 724 packets
2025-04-03: 95 packets
2025-04-04: 33 packets
2025-04-05: 188 packets
2025-04-06: 376 packets
2025-04-07: 230 packets
2025-04-08: 68 packets
2025-04-09: 131 packets
2025-04-10: 544 packets
2025-04-11: 499 packets
2025-04-12: 62 packets
2025-04-13: 219 packets
2025-04-14: 171 packets

TETRA - Terrestrial Trunked Radio Example

- TETRA is a professional mobile radio (PMR) and two-way transceiver specification
- developed by the European Telecommunications Standards Institute (ETSI).
- It's primarily used for critical communications, especially by:
  - Public safety agencies (police, fire, ambulance)
  - Military and defense
  - Utilities and transport sectors
  - Governmental organizations

  Image source: https://www.comtec-do.de/hytera-tetra/

TETRA Packet Summary

- Carrier: 47
- Header Info: 47
  - Timer: 0x6cef
  - TX Register: 0×f8fd
  - Channels: 2 TX1: 3 TX2-14
- PDU Type: 0 (MAC Resource Element)
- Encryption Mode: None
- Access Acknowledged: Yes
- Address: 7 (SMI Event Label:fd:a:15:a3:c0)
- Power Control: Level 8
- Slot Granting: Disabled
- Channel Allocation: Active
  - Timeslot: 7
  - Uplink/Downlink: Assigned
  - Cell Change: Yes
  - Carrier #: 2535

TETRA - Terrestrial Trunked Radio Example

TETRA - Terrestrial Trunked Radio Example

- 1860 unique source IP addresses
- Many scanners connecting to more than 1 destination IPs
- All source IP connecting to more than 1 destination IP addresses are considered as scanner
- 1700 source IP addresses sending tetra packets to 1 IP address of blackhole
- Most frequent message: {'tetra.carrier': '0', 'tetra.header': {'tetra.timer': '0x xx'}} where xx is a number
- Most frequent message was omitted: 176 other messages were observed
- Longest tetra packet sender: sent 902 tetra packets

TETRA - Terrestrial Trunked Radio Example

- tshark -n -r pcap -Y "ip && udp && tetra" -T json


```
"tetra": {
    "tetra.carrier": "46",
    "tetra.header": {
      "tetra.timer": "0x5050"
    }
```

Conclusions

- Default routing is a common reason for collecting data from misconfigured systems
- Misconfigurations are hard to spot in redundant and failover systems
- Protect your public facing devices as mass exploitation can happen rapidly
- Not all devices should be exposed to the internet

→ Misconfigurations may release valuable/sensitive organisation infrastructure in the wild

→ The uncontrolled information spreading may pave the way for attackers to target your systems

Conclusions

Cybersecurity is

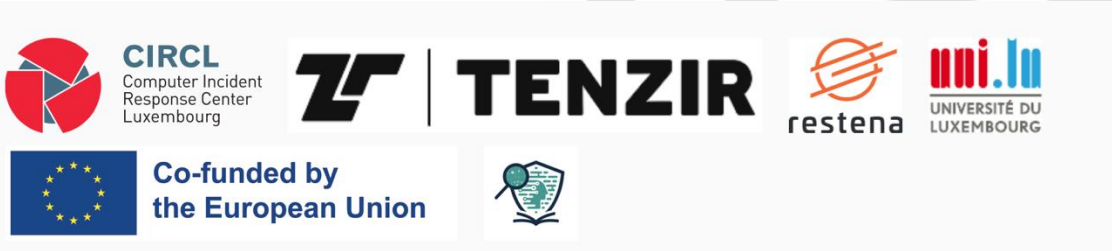
- Risk management
- Know about your assets, have control
- Is part of data control
- Having control about IT services and suppliers
- Training staff on best practices and standards

NGSOTI Project

Next Generation Security Operator Training Infrastructure (NGSOTI)

- Details
  - Project Number: 101127921
  - Project start: 01/01/2024
  - Duration: 36 Months
  - Call: DIGITAL-ECCC-2022-CYBER-03
  - Budget: 1.48 M€
- Consortium

- Objective
  - Create an open-source infrastructure for SOC operators practical training regarding network-related alerts



Any questions? Thank you !