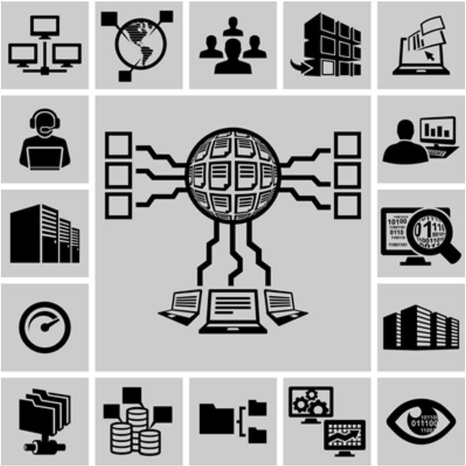
# Threat Landscape and Good Practice Guide for Internet Infrastructure

## The Physical and Logical Layers



**Dr. Cédric LÉVY-BENCHETON**

**Network and Information Security Expert**

**European Union Agency for Network and Information Security**

ENISA Workshop on EU Threat Landscape, Brussels, 24 February 2015

Follow ENISA:

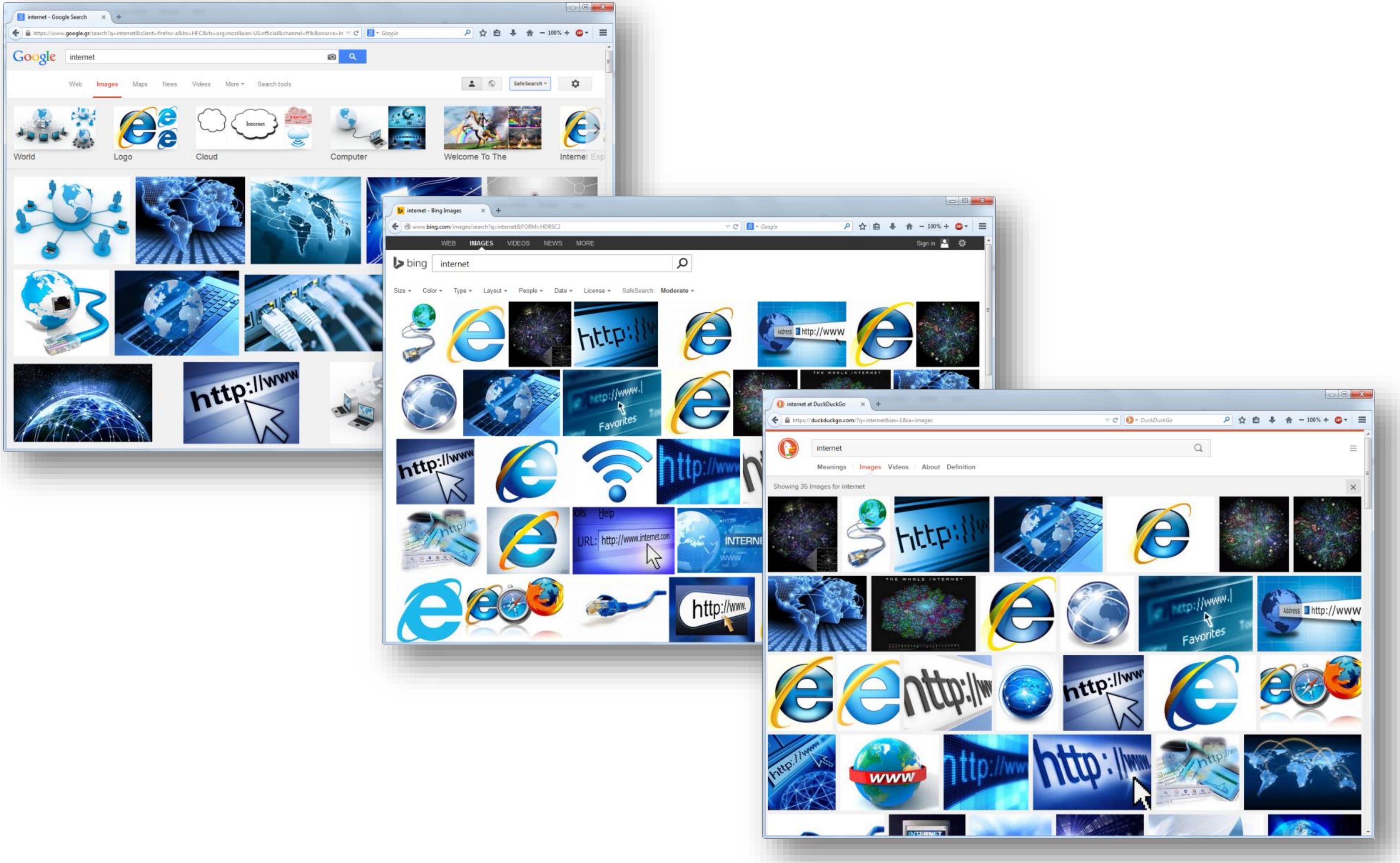
# Summary

- Introduction
- Highlights of the project
- Conclusion

# Summary

- Introduction
- Highlights of the project
- Conclusion

# What is the Internet? A very abstract thing



internet - Google Search

https://www.google.gr/search?q=internet&client=firefox-a&hs=HFC&rls=org.mozilla:en-US:official&channel=fflb&source=ln

internet

SafeSearch

internet - Bing Images

www.bing.com/images/search?q=internet&FORM=HDRSC2

internet

SafeSearch: Moderate

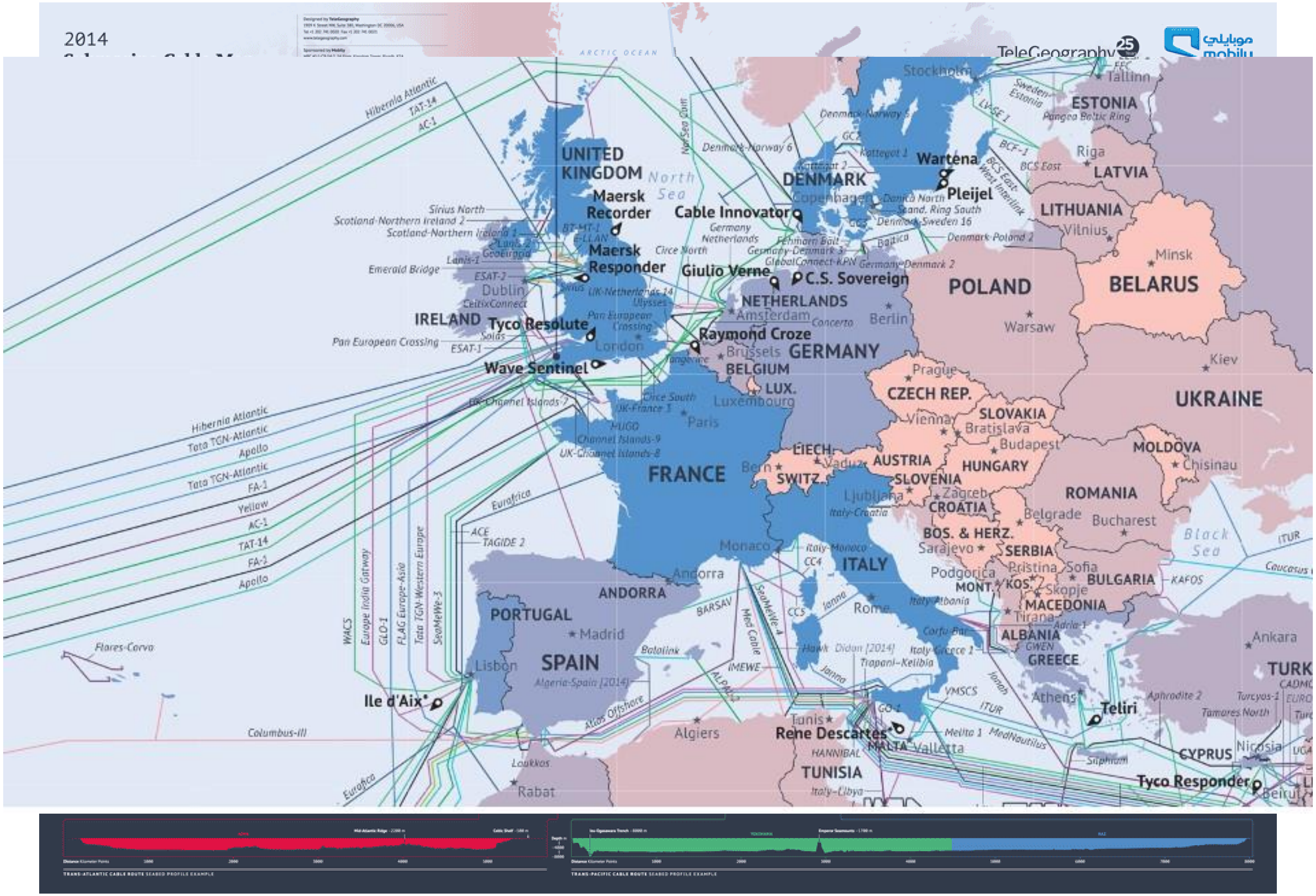
internet at DuckDuckGo

https://duckduckgo.com/?q=internet&ia=1&ia=images

internet

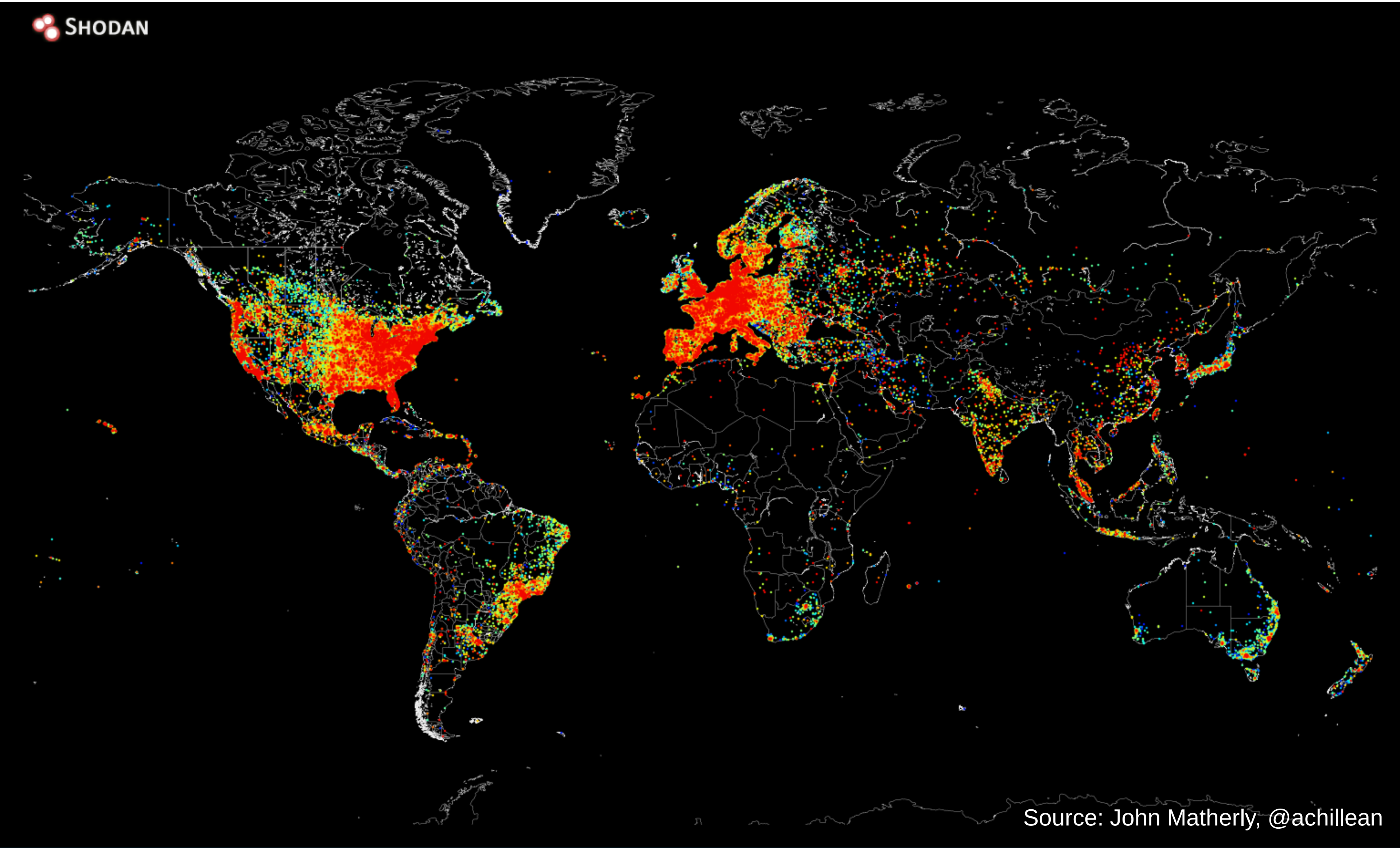
Showing 35 Images for internet

# What is the Internet? Underwater cables



Source: Telegeography

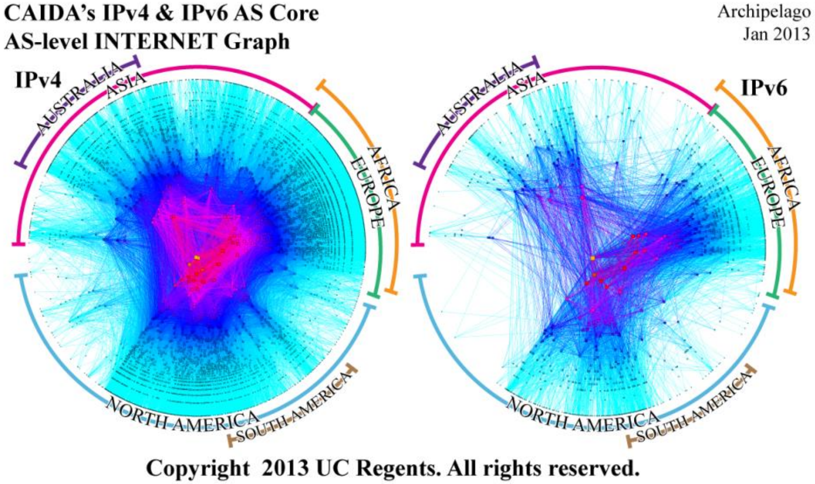
# What is the Internet? Connected devices

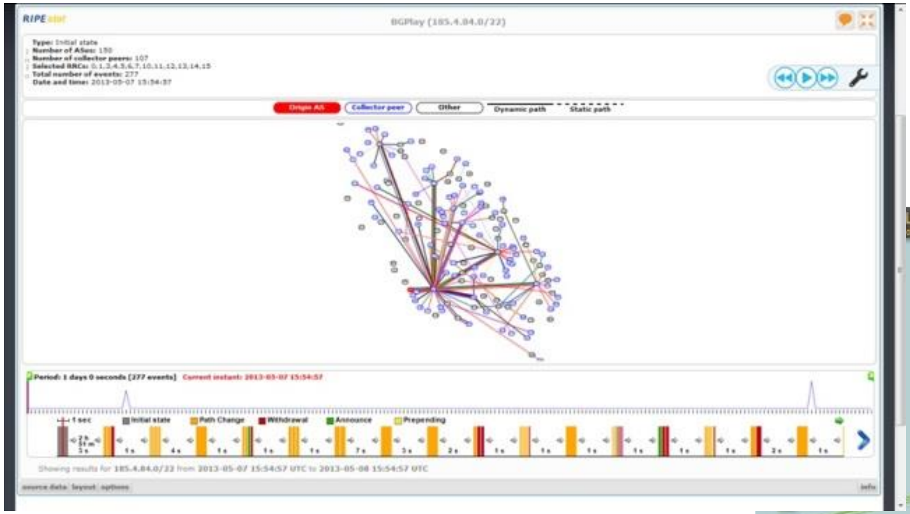


Source: John Matherly, @achillean

# What is the Internet? Logical and Physical links

- BGP-derived maps
- AS Router-Level Topologies
- PoP-Level Topologies

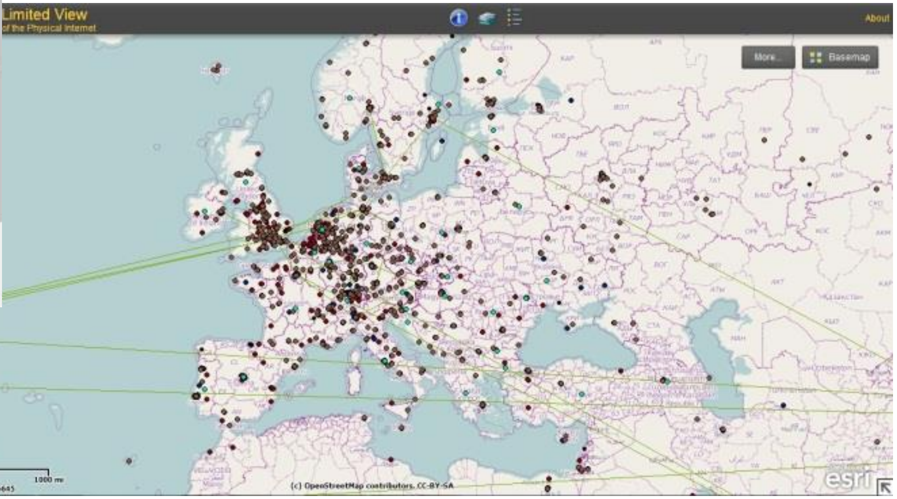




Type: Initial state
Number of ASes: 150
Number of collector peers: 107
Selected RRCs: 0,1,2,4,5,6,7,10,11,12,13,14,15
Total number of events: 277
Date and time: 2013-05-07 15:54:57

Period: 1 days 0 seconds [277 events] Current instant: 2013-05-07 15:54:57

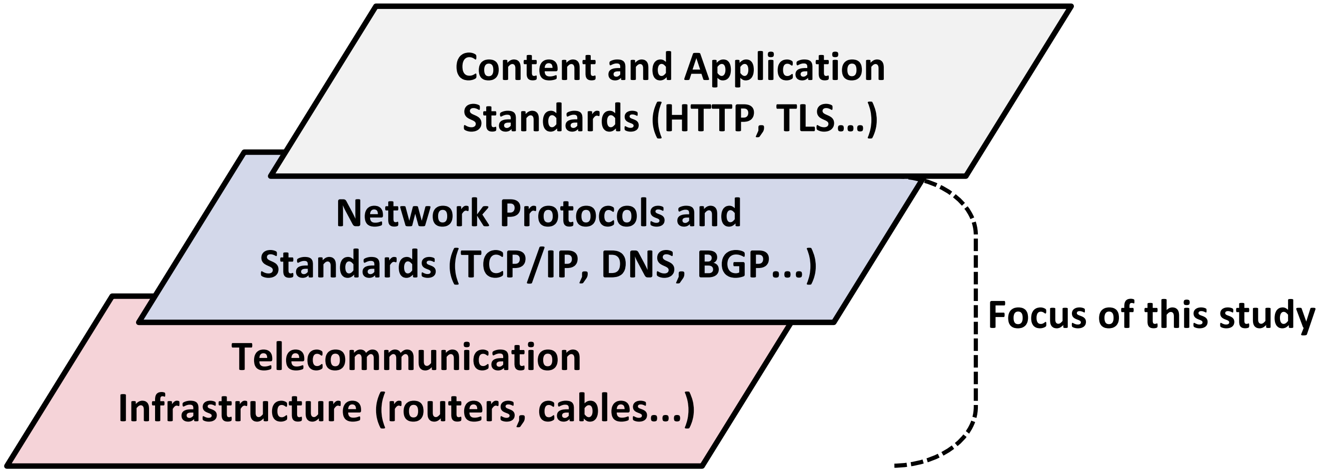
Showing results for 185.4.84.0/22 from 2013-05-07 15:54:57 UTC to 2013-05-08 15:54:57 UTC



# Scope of the project

- Definition of the Internet [RFC 2026]

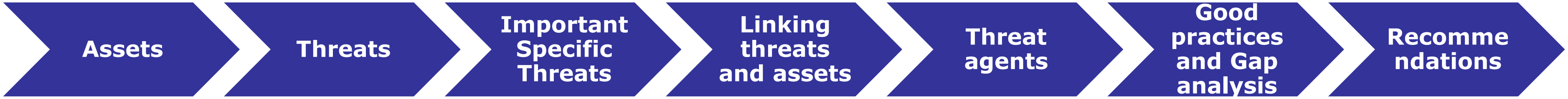
*The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards. There are also many isolated interconnected networks, which are not connected to the global Internet but use the Internet Standards.*


Content and Application Standards (HTTP, TLS…)
Network Protocols and Standards (TCP/IP, DNS, BGP...)
Telecommunication Infrastructure (routers, cables...)
Focus of this study

# Summary

- Introduction
- Highlights of the project
- Conclusion

# Content of the study



Assets

Threats

Important Specific Threats

Linking threats and assets

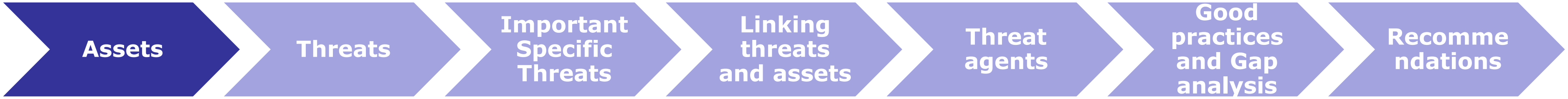
Threat agents

Good practices and Gap analysis

Recommendations

1. Identify valuable assets of physical and logical layers of the Internet infrastructure
2. Collect and evaluate information on current threats
3. Evaluate *Important Specific Threats* and assess trends
4. Link threats with assets involved
5. Link threats to the threat agents
6. Take stock of available good practices to reduce threat exposure and perform an overall gap analysis
7. Propose recommendations in protection measures

# Identify valuable assets



Assets

Threats

Important Specific Threats

Linking threats and assets

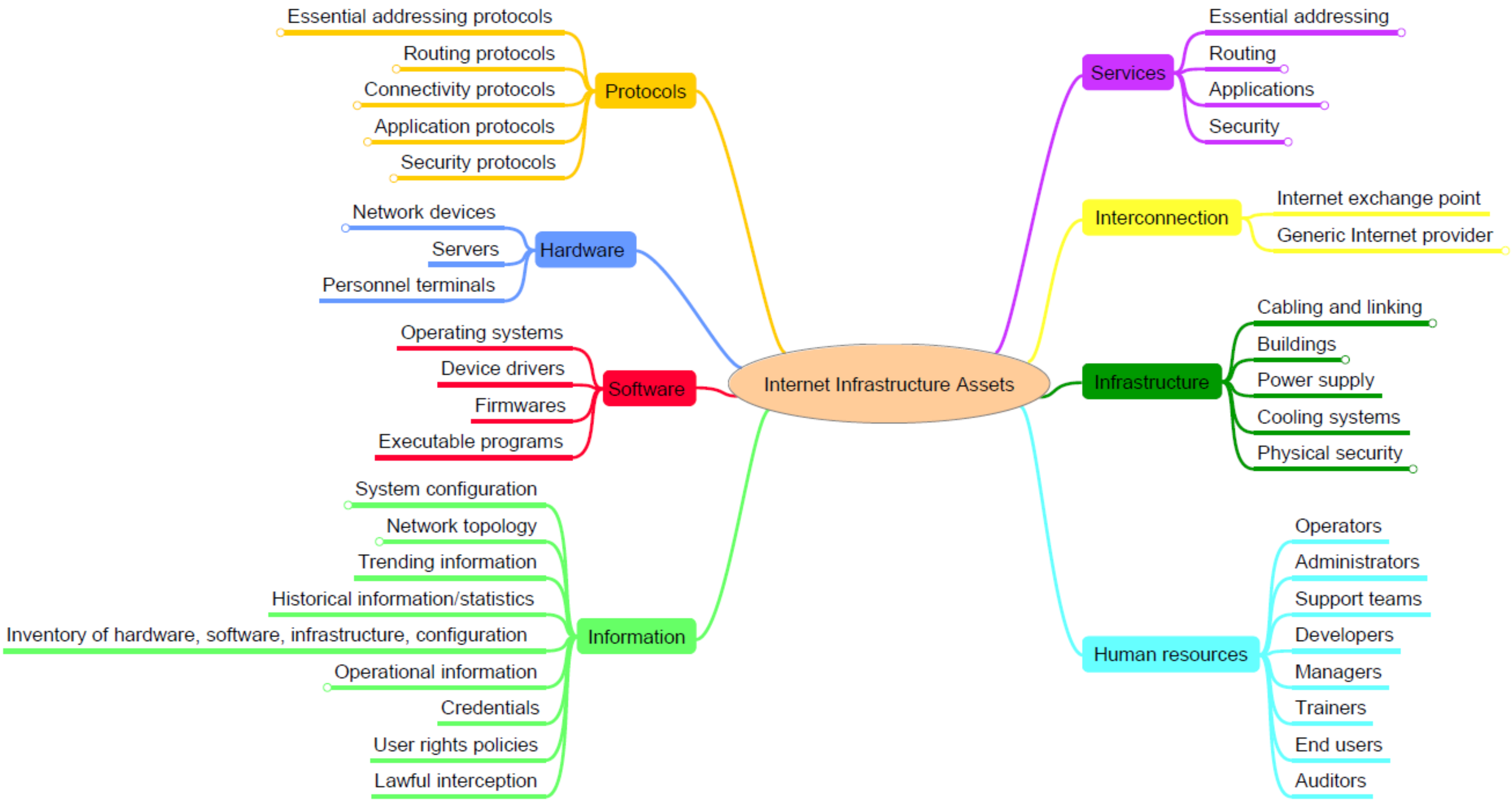
Threat agents

Good practices and Gap analysis

Recommendations

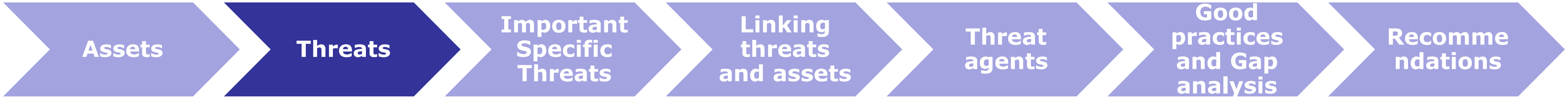
- Methodology
  - Identify assets of the Internet infrastructure
  - Structured list of **assets types**
- Results:
  - Assets mind map
- Dependencies not assessed at this stage

# Result: Assets mind map (levels 1 and 2)



- Internet Infrastructure Assets
  - Protocols
    - Essential addressing protocols
    - Routing protocols
    - Connectivity protocols
    - Application protocols
    - Security protocols
  - Hardware
    - Network devices
    - Servers
    - Personnel terminals
  - Software
    - Operating systems
    - Device drivers
    - Firmwares
    - Executable programs
  - Information
    - System configuration
    - Network topology
    - Trending information
    - Historical information/statistics
    - Inventory of hardware, software, infrastructure, configuration
    - Operational information
    - Credentials
    - User rights policies
    - Lawful interception
  - Services
    - Essential addressing
    - Routing
    - Applications
    - Security
  - Interconnection
    - Internet exchange point
    - Generic Internet provider
  - Infrastructure
    - Cabling and linking
    - Buildings
    - Power supply
    - Cooling systems
    - Physical security
  - Human resources
    - Operators
    - Administrators
    - Support teams
    - Developers
    - Managers
    - Trainers
    - End users
    - Auditors

# Identify threats



Assets

Threats

Important Specific Threats

Linking threats and assets

Threat agents

Good practices and Gap analysis

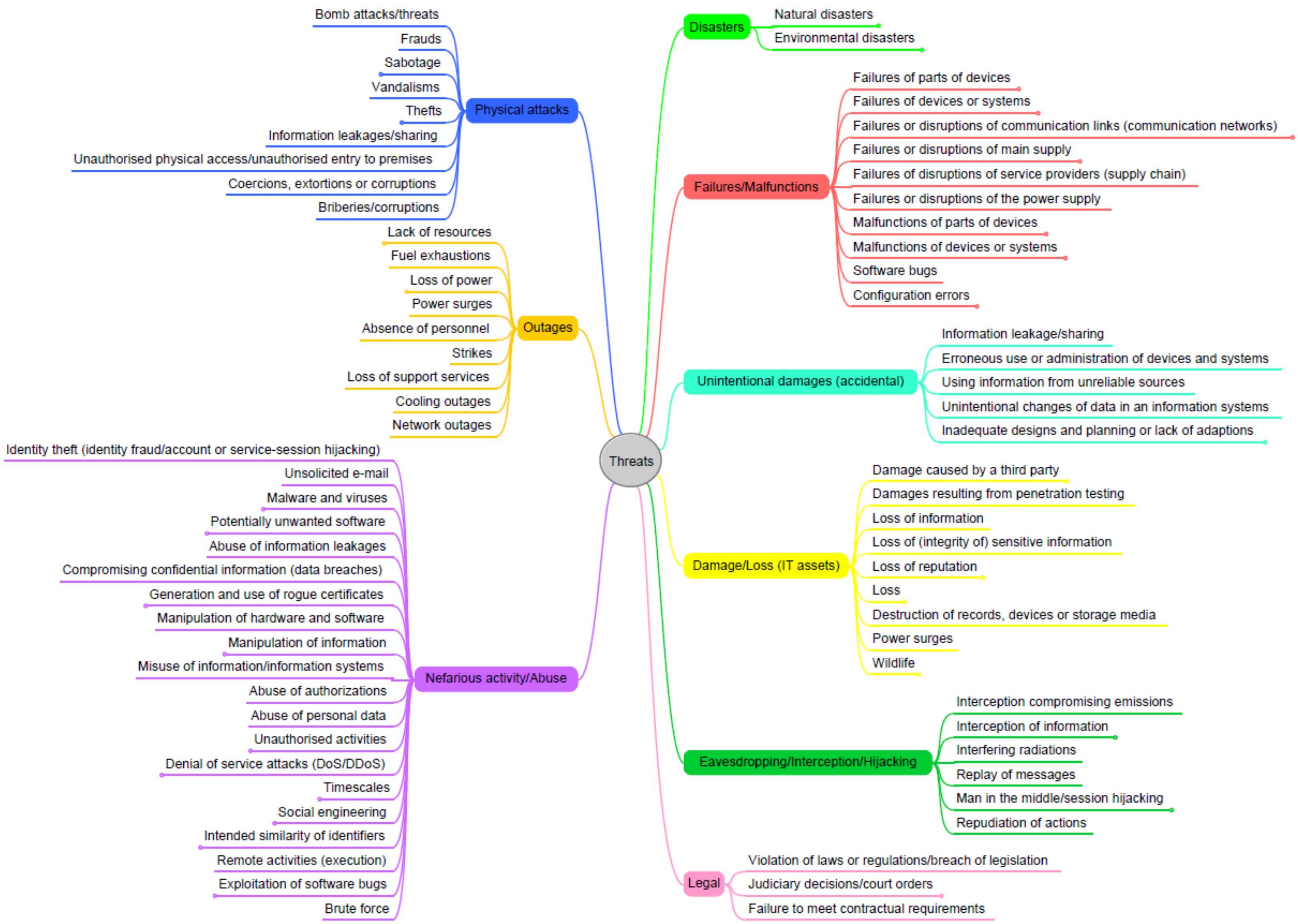
Recommendations

- Methodology
  - Identify all possible threats
  - Classify threats in **threat types**

- Results:
  - Mind maps (threats and threat agents)

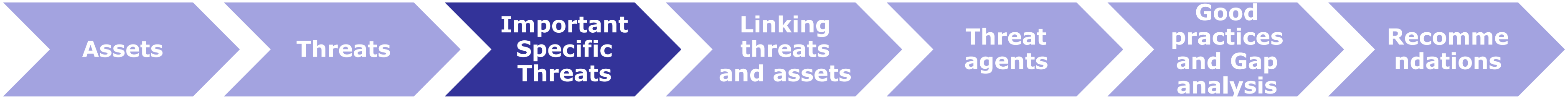
- Dependencies not assessed at this stage

# Result: Threats mind map (levels 1 and 2)



- Threats
  - Physical attacks
    - Bomb attacks/threats
    - Frauds
    - Sabotage
    - Vandalisms
    - Thefts
    - Information leakages/sharing
    - Unauthorised physical access/unauthorised entry to premises
    - Coercions, extortions or corruptions
    - Briberies/corruptions
  - Outages
    - Lack of resources
    - Fuel exhaustions
    - Loss of power
    - Power surges
    - Absence of personnel
    - Strikes
    - Loss of support services
    - Cooling outages
    - Network outages
  - Nefarious activity/Abuse
    - Identity theft (identity fraud/account or service-session hijacking)
    - Unsolicited e-mail
    - Malware and viruses
    - Potentially unwanted software
    - Abuse of information leakages
    - Compromising confidential information (data breaches)
    - Generation and use of rogue certificates
    - Manipulation of hardware and software
    - Manipulation of information
    - Misuse of information/information systems
    - Abuse of authorizations
    - Abuse of personal data
    - Unauthorised activities
    - Denial of service attacks (DoS/DDoS)
    - Timescales
    - Social engineering
    - Intended similarity of identifiers
    - Remote activities (execution)
    - Exploitation of software bugs
    - Brute force
  - Disasters
    - Natural disasters
    - Environmental disasters
  - Failures/Malfunctions
    - Failures of parts of devices
    - Failures of devices or systems
    - Failures or disruptions of communication links (communication networks)
    - Failures or disruptions of main supply
    - Failures of disruptions of service providers (supply chain)
    - Failures or disruptions of the power supply
    - Malfunctions of parts of devices
    - Malfunctions of devices or systems
    - Software bugs
    - Configuration errors
  - Unintentional damages (accidental)
    - Information leakage/sharing
    - Erroneous use or administration of devices and systems
    - Using information from unreliable sources
    - Unintentional changes of data in an information systems
    - Inadequate designs and planning or lack of adaptions
  - Damage/Loss (IT assets)
    - Damage caused by a third party
    - Damages resulting from penetration testing
    - Loss of information
    - Loss of (integrity of) sensitive information
    - Loss of reputation
    - Loss
    - Destruction of records, devices or storage media
    - Power surges
    - Wildlife
  - Eavesdropping/Interception/Hijacking
    - Interception compromising emissions
    - Interception of information
    - Interfering radiations
    - Replay of messages
    - Man in the middle/session hijacking
    - Repudiation of actions
  - Legal
    - Violation of laws or regulations/breach of legislation
    - Judiciary decisions/court orders
    - Failure to meet contractual requirements

# Important Specific Threats



Assets

Threats

Important Specific Threats

Linking threats and assets

Threat agents

Good practices and Gap analysis

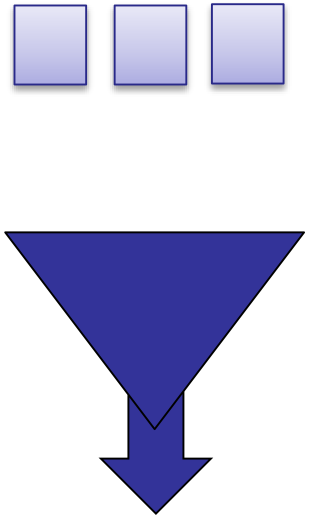
Recommendations

- Methodology
  - Desktop research from authoritative sources

- Results:
  - Classification of important specific threats into “**Threats groups**”
  - Detailed description of important specific threats with the trends

*ATTENTION: Trends increasing (resp. decreasing) only signify that the amount of specific attacks is higher (resp. lower) compared to the previous year*

# Method to identify important specific threats



Reports about threats

- – Frequency of appearance/references in reports
- – Appearance/references are estimated if no valid data was available (e.g. DDoS)
- – Expert group judgment

Filter:

- Is threat relevant for the Internet infrastructure?
- Is threat specifically highlighted as important?
- Is threat already in the list?

- A
- B
- C

Reports about threats

Reports investigated:

- “2014 Data Breach Investigations Report”, Verizon, 2014.
- “Cloud Computing Top Threats in 2013”, Cloud Security Alliance, 2013.
- “ENISA Threat Landscape Mid-year 2013”, ENISA, 2013.
- “IBM Security Services Cyber Security Intelligence Index”, IBM, 2013.
- “BSI Threats Catalogue”, Federal Office for Information Security, 2012.
- “512k Maggedon”, RIPE Labs, 2014.

Additional sources to evaluate trends:

- ENISA Threat Landscape 2013
- ENISA Annual Incident Reports 2013
- Hackmaggedon Analysis

# Result: Classification of Important Specific Threats into Threat Groups

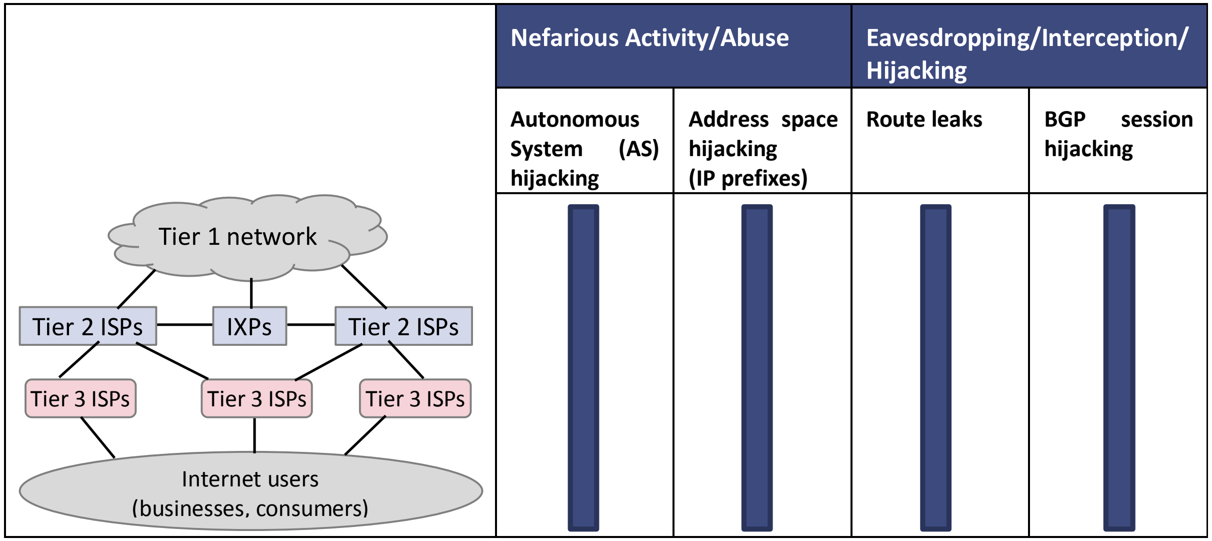
Threat Groups

- Routing Threats
  - Autonomous System (AS) hijacking
  - Address space hijacking (IP prefixes)
  - Route leaks
  - BGP session hijacking
- DNS Threats
  - DNS registrar hijacking
  - DNS spoofing
  - DNS poisoning (cache)
  - Domain name collision
- Denial of Service Threats
  - DDoS Amplification/reflection (NTP, DNS…)
  - DoS flooding (UDP, ICMP…)
  - DoS protocol exploitation (TCP-SYN, Push+Ack, …)
  - DoS malformed packet attack (IP address options, …)
  - DoS application (XDoS, …)
- Generic Threats
  - Physical attack
  - Damage/loss
  - Failure of devices or systems
  - Configuration errors
  - Malware and virus (botnet…)
  - Brute force
  - Social engineering
  - Data breach
  - Espionage

# Result: Routing threats

- Nefarious Activity/Abuse — Trend: Increasing ↑
  - Autonomous System (AS) hijacking
  - Address space hijacking (IP prefixes)

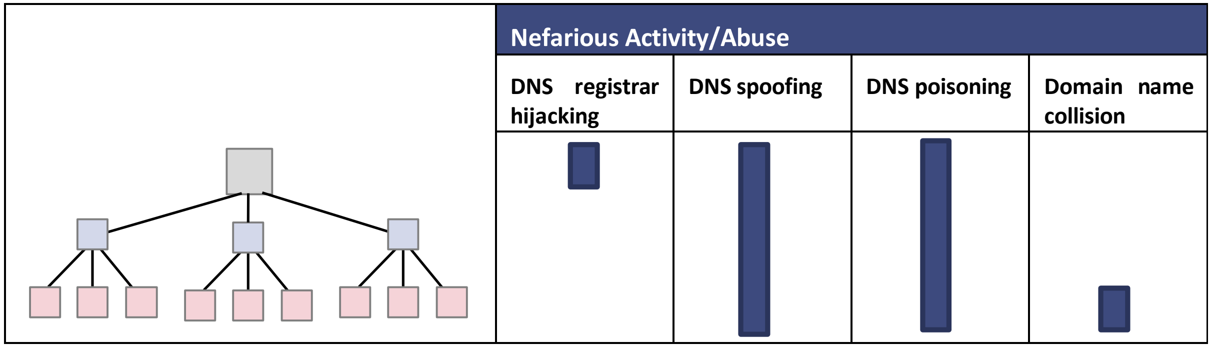
- Eavesdropping/Interception/Hijacking — Trend: Increasing ↑
  - Route leaks
  - BGP session hijacking



| Nefarious Activity/Abuse | | Eavesdropping/Interception/ Hijacking | |
|---|---|---|---|
| Autonomous System (AS) hijacking | Address space hijacking (IP prefixes) | Route leaks | BGP session hijacking |
| ▮ | ▮ | ▮ | ▮ |

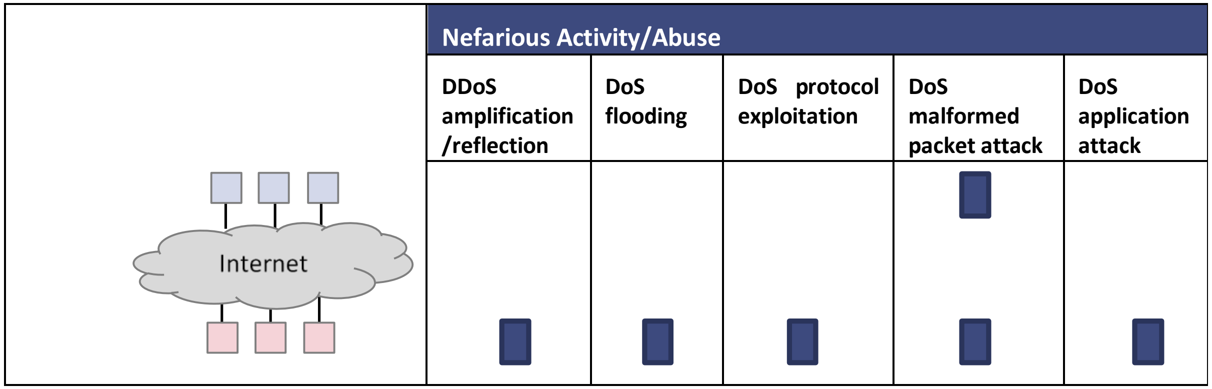
# Result: DNS threats

- Threat type: Nefarious Activity/Abuse — Trend: Decreasing ⬇
  - DNS registrar hijacking
  - DNS spoofing
  - DNS poisoning (cache)
  - Domain name collision



# Result: Denial of Service threats

- Threat Type: Nefarious Activity/Abuse Trend: Increasing ⇧
  - DDoS amplification/reflection (NTP, DNS…)
  - DoS flooding (UDP, ICMP…)
  - DoS protocol exploitation (TCP-SYN, Push+Ack, …)
  - DoS malformed packet attack (IP address options, …)
  - DoS application (XDoS, …)



| Nefarious Activity/Abuse | | | | |
|---|---|---|---|---|
| DDoS amplification /reflection | DoS flooding | DoS protocol exploitation | DoS malformed packet attack | DoS application attack |
| | | | ■ | |
| ■ | ■ | ■ | ■ | ■ |

# Result: Generic threats

| | |
|---|---|
| • Physical attack | Trend: N/A |
| • Damage/Loss | Trend: Increasing ↑ |
| • Failures/Malfunctions | Trend: Increasing ↑ |
| – Failure of devices or systems | |
| – Configuration errors | |
| • Nefarious activity/Abuse | Trend: Increasing ↑ |
| – Malware and virus (botnet…) | |
| – Brute force | |
| – Social engineering | |
| – Data breach | |
| • Eavesdropping/Interception/Hijacking | Trend: Increasing ↑ |
| – Espionage | |

# Result: Summary of trends

| Threat groups | Threat types | Trends |
|---|---|---|
| **Routing Threats** | Nefarious Activity/Abuse | Increasing ⬆ |
| | Eavesdropping/Interception/Hijacking | Increasing ⬆ |
| **DNS Threats** | Nefarious Activity/Abuse | Decreasing ⬇ |
| **Denial of Service** | Nefarious Activity/Abuse | Increasing ⬆ |
| **Generic Threats** | Physical attack | N/A |
| | Damage/Loss | Increasing ⬆ |
| | Failures/Malfunctions | Increasing ⬆ |
| | Nefarious activity/Abuse | Increasing ⬆ |
| | Eavesdropping/Interception/Hijacking | Increasing ⬆ |

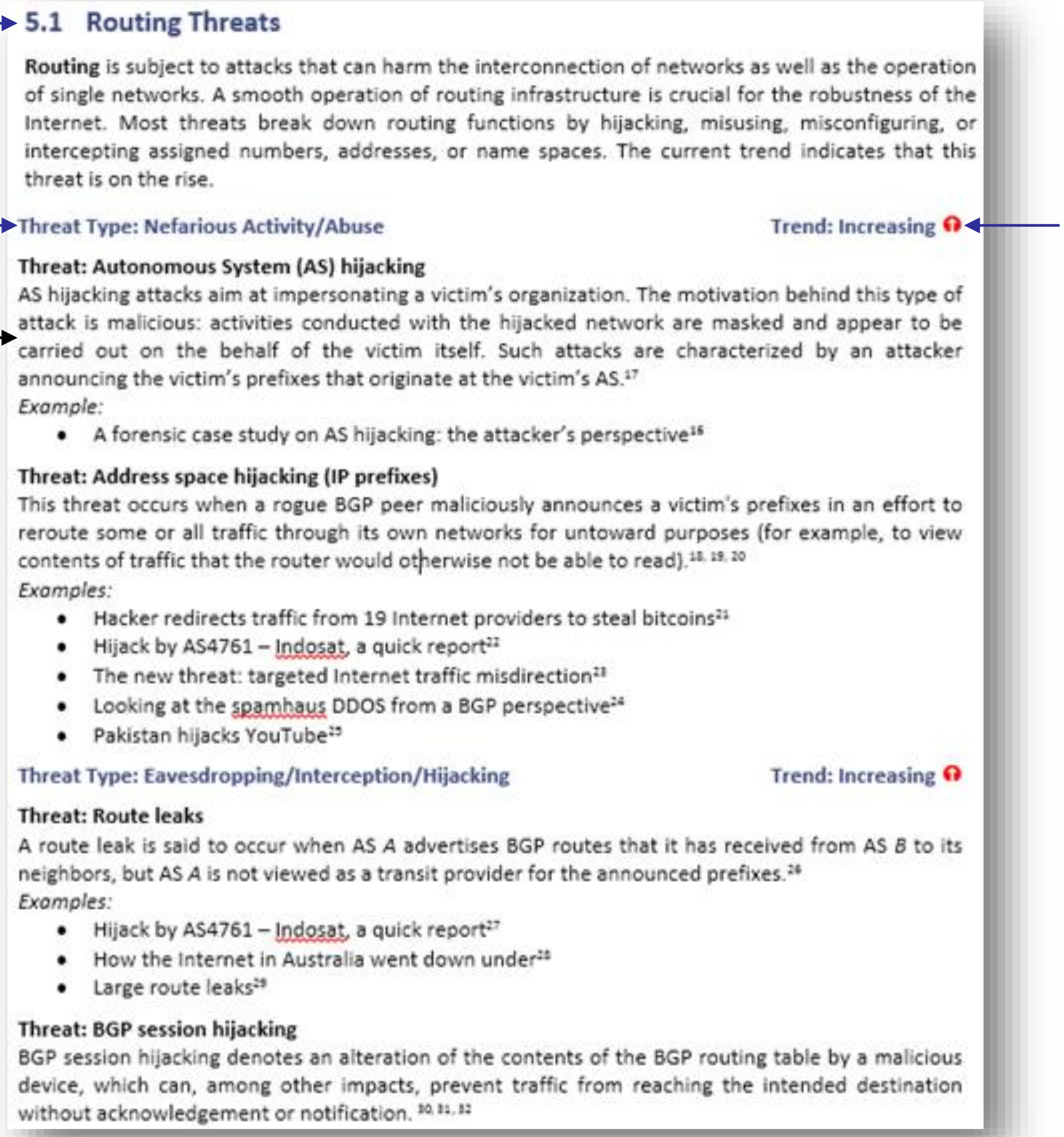
# Result: Description of important specific threats with trends (excerpt)

Threat groups →

Threat type (mind map) →

Threat description →

← Threat trend



### 5.1 Routing Threats

**Routing** is subject to attacks that can harm the interconnection of networks as well as the operation of single networks. A smooth operation of routing infrastructure is crucial for the robustness of the Internet. Most threats break down routing functions by hijacking, misusing, misconfiguring, or intercepting assigned numbers, addresses, or name spaces. The current trend indicates that this threat is on the rise.

Threat Type: Nefarious Activity/Abuse — Trend: Increasing ↑

**Threat: Autonomous System (AS) hijacking**

AS hijacking attacks aim at impersonating a victim's organization. The motivation behind this type of attack is malicious: activities conducted with the hijacked network are masked and appear to be carried out on the behalf of the victim itself. Such attacks are characterized by an attacker announcing the victim's prefixes that originate at the victim's AS.[17]

*Example:*

- A forensic case study on AS hijacking: the attacker's perspective[16]

**Threat: Address space hijacking (IP prefixes)**

This threat occurs when a rogue BGP peer maliciously announces a victim's prefixes in an effort to reroute some or all traffic through its own networks for untoward purposes (for example, to view contents of traffic that the router would otherwise not be able to read).[18, 19, 20]

*Examples:*

- Hacker redirects traffic from 19 Internet providers to steal bitcoins[21]
- Hijack by AS4761 – Indosat, a quick report[22]
- The new threat: targeted Internet traffic misdirection[23]
- Looking at the spamhaus DDOS from a BGP perspective[24]
- Pakistan hijacks YouTube[25]

Threat Type: Eavesdropping/Interception/Hijacking — Trend: Increasing ↑

**Threat: Route leaks**

A route leak is said to occur when AS *A* advertises BGP routes that it has received from AS *B* to its neighbors, but AS *A* is not viewed as a transit provider for the announced prefixes.[26]

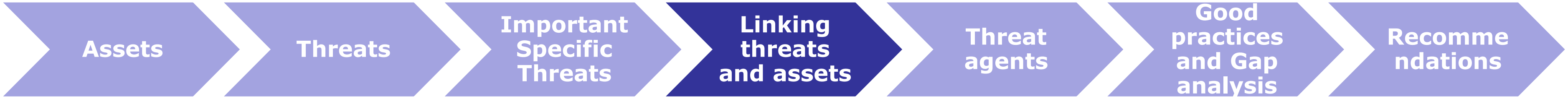
*Examples:*

- Hijack by AS4761 – Indosat, a quick report[27]
- How the Internet in Australia went down under[28]
- Large route leaks[29]

**Threat: BGP session hijacking**

BGP session hijacking denotes an alteration of the contents of the BGP routing table by a malicious device, which can, among other impacts, prevent traffic from reaching the intended destination without acknowledgement or notification.[30, 31, 32]

# Linking threats and assets


Assets

Threats

Important Specific Threats

Linking threats and assets

Threat agents

Good practices and Gap analysis

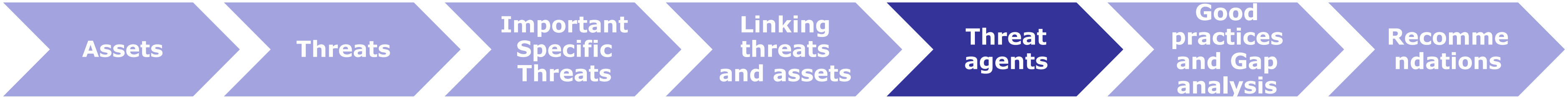
Recommendations

- Methodology
  - Link the threats with the assets involved (1-to-N mapping)
  - Limit to a certain level of the mind map (not too detailed)
- Results:
  - Description of the asset types involved in every threat

# Result: Linking threats with assets involved (excerpt)

| Threat types | Threats | Asset types |
|---|---|---|
| **Physical attacks** | Information leakages/sharing | Information, Infrastructure, Interconnection |
| **Unintentional damages (accidental)** | Erroneous use or administration of devices and systems | Protocols, Hardware, Software, Information, Services |
| **Failures/Malfunctions** | Failures of disruptions of service providers (supply chain) | Protocols, Hardware, Software, Information, Services |
| **Disasters** | Natural disasters | Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources |
| **Outages** | Network outages | Hardware, Software, Information, Services |
| **Damage/Loss (IT assets)** | Damage caused by a third parties | Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources |
| **Eavesdropping/Interception/Hijacking** | Man in the middle/session hijacking | Software, Information, Services |
| **Legal** | Violations of law or regulation/breaches of legislation | Software, Information, Interconnection, Human resoures |
| **Nefarious activity/Abuse** | Misuse of information/information systems | Protocols, Hardware, Software, Information, Services, Interconnection |
| | Denial of service attacks (DoS/DDoS) | Hardware, Software, Information, Services |

# Threat agents



Assets

Threats

Important Specific Threats

Linking threats and assets

Threat agents

Good practices and Gap analysis

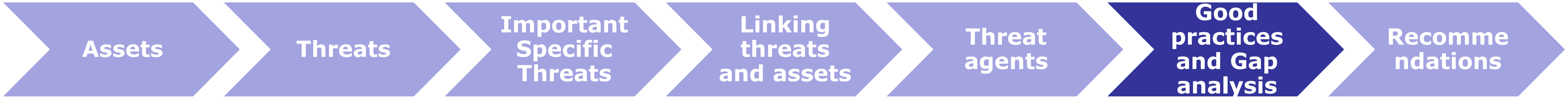
Recommendations

- Methodology
  - Threat agents mapped in "ENISA Threat Landscape 2013"
  - Evaluate of threat agents for every threat type
- Results:
  - Presentation of the threat agents involved for every threat type

# Result: Involvement of threat agents in threats

| | Corporations | Hacktivists | Cyber criminals | Cyber terrorists | Script kiddies | Online social hackers | Employees | Nations states |
|---|---|---|---|---|---|---|---|---|
| Physical attacks | ✓ | - | ✓ | ✓ | - | - | ✓ | ✓ |
| Disasters | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| Failures/ Malfunctions | ✓ | - | - | - | - | - | ✓ | - |
| Outages | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Unintentional damages | ✓ | - | - | - | - | - | ✓ | - |
| Damage/Loss | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Nefarious activity/Abuse | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Eavesdropping/ Interception/ Hijacking | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Legal | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# Good practices and Gap analysis



Assets

Threats

Important Specific Threats

Linking threats and assets

Threat agents

Good practices and Gap analysis

Recommendations

- Methodology
  - Desktop research from authoritative sources
  - Interview with experts
  - Identify assets not covered by at least one good practice

- Results
  - Description of good practices to mitigate each threat
  - Coverage of assets for every good practice presented
  - Gap analysis: assets not covered

# Methodology: List of sources and experts

## 1. Good practices from different organisations

- RIPE
- APNIC
- ARIN
- LACNIC
- AFRINIC
- CENTR
- DNS-OARC
- NANOG
- PACNOG
- IETF
- NIST
- Route Manifesto
- ICANN
- CISCO
- Juniper
- BSI
- ENISA
- Euro-IX
- Internet Society
- Cisesecurity.org
- Bettercrypto.org

## 2. Experts contacted

- Peter Koch (DNS)
- Patrik Falstrom (DNS)
- Benno Overeinder (Routing / BGP)
- Andrei Robachevsky (Routing / BGP)
- Randy Bush (RPKI / Routing)

# Result: Good practices against routing threats (excerpt)

| Threats | Good practices | Assets, assets covered | Gaps |
|---|---|---|---|
| **AS Hijacking** | | Internet protocol addressing, Routing protocols, Administrators | Administrators |
| | Utilise resource certification (RPKI) to provide AS origin validation. Reader must be aware that at the time of writing, it is no possible to detect AS hijacking automatically. | Internet protocol addressing, Routing protocols | Administrators |
| **Address space hijacking (IP prefixes)** | | Routing, Internet protocol addressing, System configurations, Network topology | - |
| | Registry databases such as IRR, APNIC, ARIN, and RIPE have to be subject to continuous maintenance. This shall allow usage of updated information to secure peering. For example, the “Route Object” field can help validating routes received from peers. | Routing, Internet protocol addressing, System configurations | Network topology |
| | Configuration updates for the routing infrastructure may only be performed by a defined authority using strong authentication. | Routing, System configurations, Network topology | Internet protocol addressing |
| **Route leaks** | | Routing, Network topology | - |
| | Configure BGP maximum-prefix to ensure the validity of routes announced. If more prefixes are received, it is sign of an incorrect behaviour and the BGP session shuts down. | Routing, Network topology | |
| **BGP session hijacking** | | Routing, Internet protocol addressing, System configurations, Network topology | - |
| | Employ AS path filtering. | Routing, Internet protocol addressing, System configurations, Network topology | |
| | Use TCP-AO (TCP-Authentication Option) to secure BGP Authentication in order to replace TCP-MD5. TCP-AO simplifies the exchange of keys. | Routing, Internet protocol addressing, System configurations, Network topology | |

# Result: Good practices against DNS threats (excerpt)

| Threats | Good practices | Assets, assets covered | Gaps |
|---|---|---|---|
| **DNS registrar hijacking** | - | Domain name system, Addressing units, Applications, Credentials, Administrators | - |
| | Registrants must protect account credentials and define authorised users, while registrars have to provide a secure authentication process. | Addressing units, Credentials, Administrators | Domain name system, Applications |
| | Registrars should consider supporting DNSSEC. | Domain name system, Addressing units, Applications | Credentials, Administrators |
| **DNS spoofing** | | Domain name system, Addressing units, Applications, System configurations, Essential addressing protocols – DNS, Administrators | Administrators |
| | Deploying DNSSEC aims to secure DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity. | Domain name system, addressing units, Applications, System Configurations, Essential addressing protocols – DNS | Administrators |
| **DNS poisoning** | | Domain name system, Addressing units, Applications, System configurations, Executable programs, Essential addressing protocols – DNS, Administrators, Operators | Administrators, Operators |
| | Restrict dynamic updates to only authorised sources in order to avoid misuse. Such misuse include the abuse of a DNS server as an amplifier, DNS cache poisoning… | Addressing units, applications, System configurations, Executable programs | Domain name system, Essential addressing protocols – DNS, Administrators, Operators |
| **Domain name collision** | | Domain name system, applications | - |
| | Preventing DNS request for internal namespaces to leak into the Internet by applying firewall policies. | Applications | Domain name system |
| | Use reserved TLDs such as .test, .example, .invalid, or .localhost. | Domain name system, Applications | |

# Result: Good practices against Denial of Service

| Threats | Good practices | Assets, assets covered | Gaps |
|---|---|---|---|
| **Amplification / reflection** | - | Applications, security, Generic Internet provider, Hardware, Executable programs, System configuration, Application protocols, Administrators, Operators | System configuration, Essential addressing protocols, Administrators, Operators |
|  | Adopt source IP address verification at the edge of Internet infrastructure (close to the origin of traffic) to prevent network address spoofing through ingress and egress filtering. | Applications, Security, Generic Internet provider, Hardware, Executable programs, Application protocols | System configuration, Administrators, Operators |
|  | Operators of authoritative name server operator should implement RRL (Response Rate Limiting). | Applications, Security, Generic Internet provider, Hardware, Executable programs | System configuration, Application protocols, Administrators, Operators |
| **Flooding** |  | Applications, Security, Generic Internet providers, Hardware, Executable programs, System configuration, Essential addressing protocols, Administrators, Operators | System configuration, Essential addressing protocols, Administrators, Operators |
|  | Manufacturers and configurators of network equipment should take steps to secure all devices and have to keep them up-to-date. | Applications, Security, Generic Internet providers, Hardware, Executable programs | System configuration, Essential addressing protocols, Administrators, Operators |
| **Protocol exploitation** | - | *Ditto* | - |
| **Malformed packet attack** | - | *Ditto* | - |
| **Application** | - | Applications, Security, Generic Internet provider, Hardware, Executable programs, System configuration, Application protocols, Administrators, Operators | - |

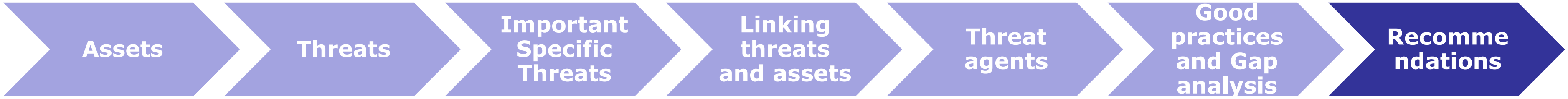
# Result: Gaps found

- Routing Threats
  - *Administrators*

- DNS
  - DNS Spoofing: *Administrators*
  - DNS Poisoning: *Administrators, Operators*

- Denial of Service / Flooding
  - *System configuration*
  - *Essential addressing protocols*
  - *Administrators*
  - *Operators*

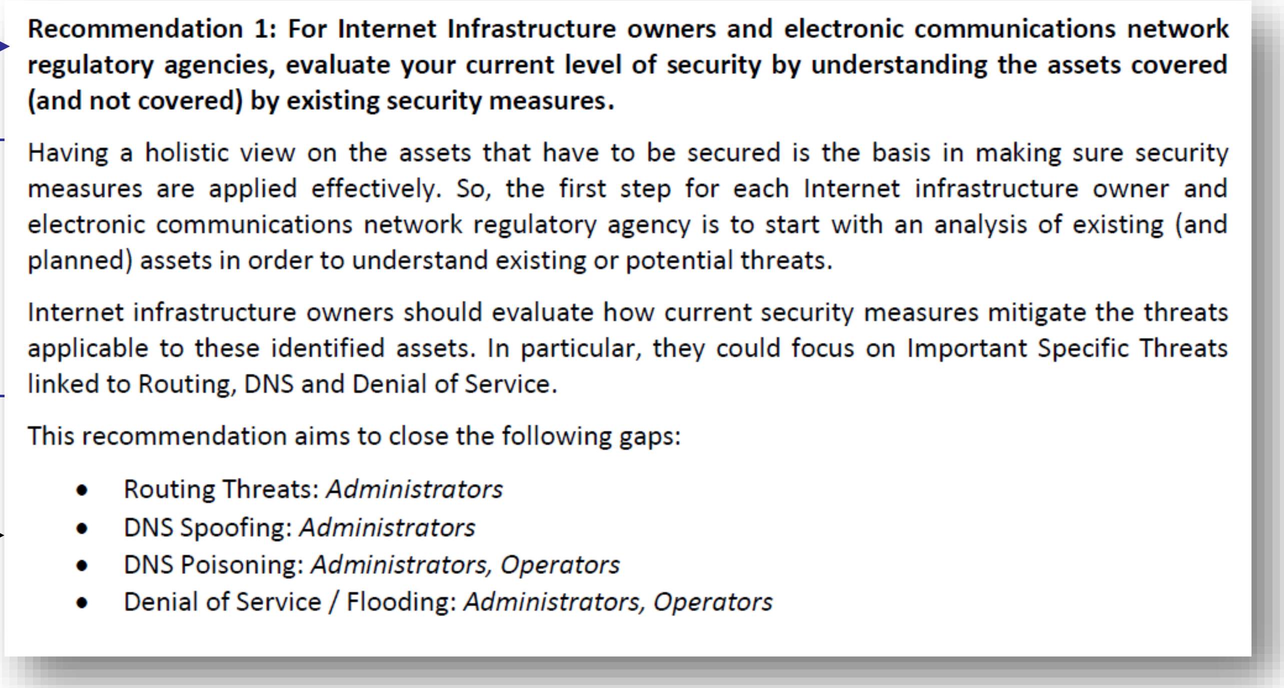
# Recommendations


Assets
Threats
Important Specific Threats
Linking threats and assets
Threat agents
Good practices and Gap analysis
Recommendations

- Methodology
  - Recommendations derived from the gap analysis
  - Validation through experts

- Results
  - Technical and organizational recommendations
  - Incentives on why the recommendation in important

# Recommendations



Recommendation →

**Recommendation 1: For Internet Infrastructure owners and electronic communications network regulatory agencies, evaluate your current level of security by understanding the assets covered (and not covered) by existing security measures.**

Description →

Having a holistic view on the assets that have to be secured is the basis in making sure security measures are applied effectively. So, the first step for each Internet infrastructure owner and electronic communications network regulatory agency is to start with an analysis of existing (and planned) assets in order to understand existing or potential threats.

Internet infrastructure owners should evaluate how current security measures mitigate the threats applicable to these identified assets. In particular, they could focus on Important Specific Threats linked to Routing, DNS and Denial of Service.

Gaps covered →

This recommendation aims to close the following gaps:

- Routing Threats: *Administrators*
- DNS Spoofing: *Administrators*
- DNS Poisoning: *Administrators, Operators*
- Denial of Service / Flooding: *Administrators, Operators*

# Result: Technical recommendations

1. For Internet Infrastructure owners and electronic communications network regulatory agencies, evaluate your current level of security by understanding the assets covered (and not covered) by existing security measures
   - For routing threats, DNS threats, Denial of Service

2. For Internet infrastructure owners, evaluate the application of adapted good practices in a focused manner

3. For Internet infrastructure owners, cooperate with the community to exchange on threats and promote the application of good practices as mitigation measures
   - Trust-based group / legal obligation, ISACs

4. For users deploying good practices guides, report on their implementations, assets covered and gaps found

5. Words matter: Ensure the right use of terms and definitions.

# Result: Organisational recommendations

6. For Internet infrastructure owners, use proper risk assessment methods to understand vulnerable assets in your Internet infrastructure and prioritise your protection actions

7. Build an information and communication technology security awareness and training program

8. Internet infrastructure owners shall commit third-party vendors to apply security measures

9. Stay current on any updates

# Summary

- Introduction
- Highlights of the project
- Conclusion

# Conclusions

- Project outcome
  - Mind maps (assets and threats)
  - Identification of trends
  - Compilation of good practices
  - Gap analysis
  - Recommendations

- Provide tools to Internet Infrastructure owners
  - Part of their risk assessment
  - Evaluate the application of threats
  - Assess the deployment of good practices

# Thank you
# Questions?

**Dr. Cédric LÉVY-BENCHETON**

cedric.levy-bencheton@enisa.europa.eu

Phone: +30 2814 409 630

Mobile: +30 6948 460 133

Follow ENISA: