Critical BGP Prefixes: A Measurement-based Analysis on Critical Infrastructure Security

Savvas Kastanakis[1,2], Shyam Krishna Khadka[1,2], Ebrima Jaw[1,2], Cristian Hesselman[1,2,3]

1 DACS Design and Analysis of Communication Systems

2 UNIVERSITY OF TWENTE.

3 SIDN LABS

NWO RESPONSIBLE INTERNET UPIN

The Internet is a Network of Networks…

The Internet is a Network of Networks…

- (1) Each network (termed Autonomous System or AS) manages its own set of IP prefixes (blocks of IP addresses).

The Internet is a Network of Networks…

(1) Each network (termed Autonomous System or AS) manages its own set of IP prefixes (blocks of IP addresses).

(2) Using the Border Gateway Protocol (**BGP**), an AS advertises routes/paths towards its prefixes to its neighboring ASes, which propagate them further. This allows all ASes on the Internet to eventually learn how to reach every prefix on the Internet.

The Internet is a Network of Networks…

(1) Each network (termed Autonomous System or AS) manages its own set of IP prefixes (blocks of IP addresses).

(2) Using the Border Gateway Protocol (**BGP**), an AS advertises routes/paths towards its prefixes to its neighboring ASes, which propagate them further. This allows all ASes on the Internet to eventually learn how to reach every prefix on the Internet.

(3) BGP was introduced almost 3 decades ago where there were a few ASes and network operators (probably) knew each other, so, **there was no need to built in trust to the BGP**.

The Internet is a Network of Networks…

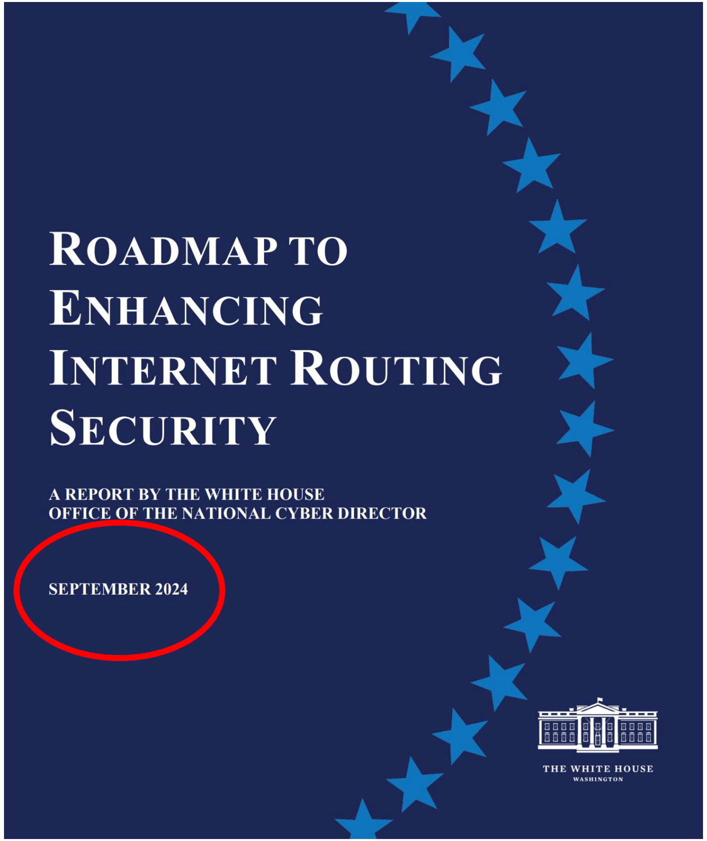
(1) Each network (termed Autonomous System or AS) manages its own set of IP prefixes (blocks of IP addresses).

(2) Using the Border Gateway Protocol (**BGP**), an AS advertises routes/paths towards its prefixes to its neighboring ASes, which propagate them further. This allows all ASes on the Internet to eventually learn how to reach every prefix on the Internet.

(3) BGP was introduced almost 3 decades ago where there were a few ASes and network operators knew each other, so, **there was no need to built in trust to the BGP**.

(4) Due to this inherent limitation (lack of built-in trust), BGP currently suffers from a variety of attacks such as ***Prefix Hijacks*** and ***Route Leaks*** (mitm, dos, impersonation).

The (zombie) roadmap to enhancing Internet routing security

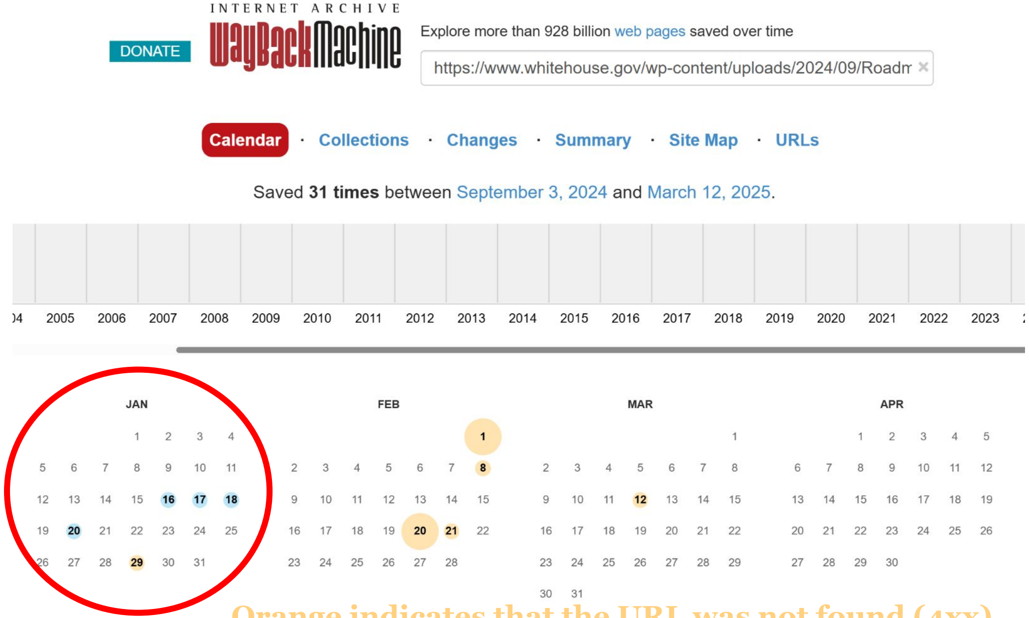


ROADMAP TO ENHANCING INTERNET ROUTING SECURITY

A REPORT BY THE WHITE HOUSE
OFFICE OF THE NATIONAL CYBER DIRECTOR

SEPTEMBER 2024

THE WHITE HOUSE
WASHINGTON



DONATE

INTERNET ARCHIVE WaybackMachine

Explore more than 928 billion web pages saved over time

https://www.whitehouse.gov/wp-content/uploads/2024/09/Roadm

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved **31 times** between September 3, 2024 and March 12, 2025.

04 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

JAN

			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

FEB

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	

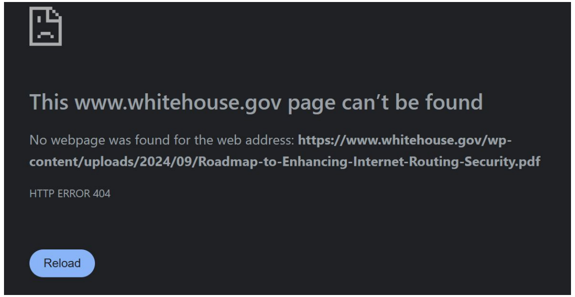
MAR

						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

APR

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Orange indicates that the URL was not found (4xx).



This www.whitehouse.gov page can’t be found

No webpage was found for the web address: **https://www.whitehouse.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf**

HTTP ERROR 404

A first-look into the roadmap

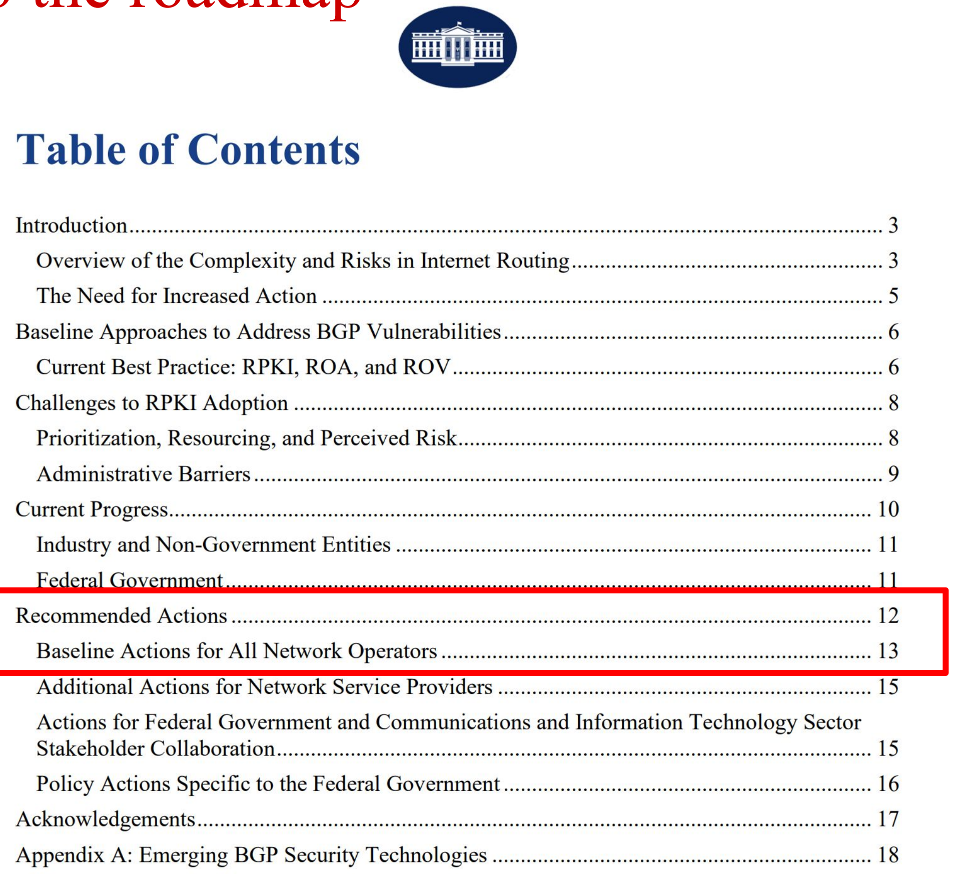


Table of Contents

Introduction 3

Overview of the Complexity and Risks in Internet Routing 3

The Need for Increased Action 5

Baseline Approaches to Address BGP Vulnerabilities 6

Current Best Practice: RPKI, ROA, and ROV 6

Challenges to RPKI Adoption 8

Prioritization, Resourcing, and Perceived Risk 8

Administrative Barriers 9

Current Progress 10

Industry and Non-Government Entities 11

Federal Government 11

Recommended Actions 12

Baseline Actions for All Network Operators 13

Additional Actions for Network Service Providers 15

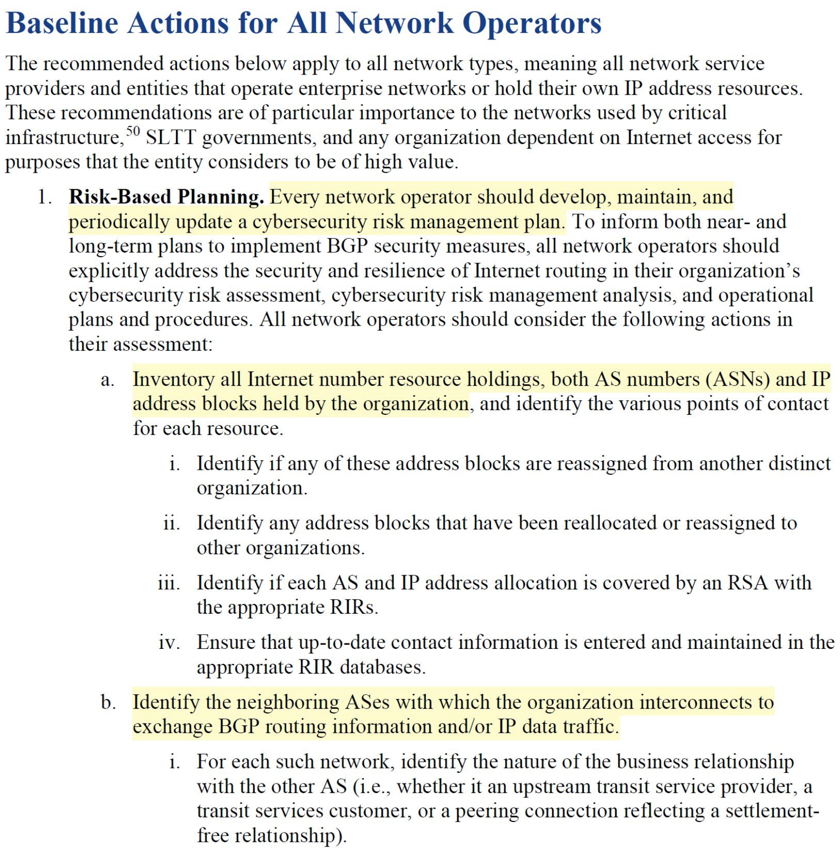
Actions for Federal Government and Communications and Information Technology Sector Stakeholder Collaboration 15

Policy Actions Specific to the Federal Government 16

Acknowledgements 17

Appendix A: Emerging BGP Security Technologies 18

Risk-based Planning for NetOps



Baseline Actions for All Network Operators

The recommended actions below apply to all network types, meaning all network service providers and entities that operate enterprise networks or hold their own IP address resources. These recommendations are of particular importance to the networks used by critical infrastructure,[50] SLTT governments, and any organization dependent on Internet access for purposes that the entity considers to be of high value.

1. **Risk-Based Planning.** Every network operator should develop, maintain, and periodically update a cybersecurity risk management plan. To inform both near- and long-term plans to implement BGP security measures, all network operators should explicitly address the security and resilience of Internet routing in their organization's cybersecurity risk assessment, cybersecurity risk management analysis, and operational plans and procedures. All network operators should consider the following actions in their assessment:

   a. Inventory all Internet number resource holdings, both AS numbers (ASNs) and IP address blocks held by the organization, and identify the various points of contact for each resource.

      i. Identify if any of these address blocks are reassigned from another distinct organization.

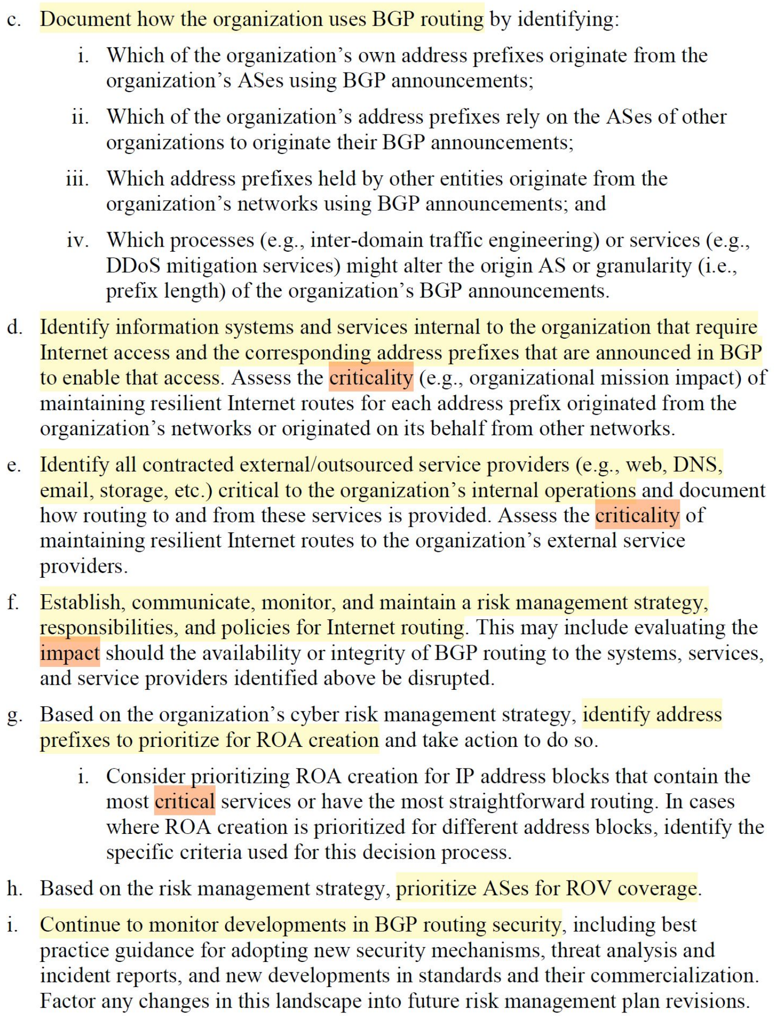
      ii. Identify any address blocks that have been reallocated or reassigned to other organizations.

      iii. Identify if each AS and IP address allocation is covered by an RSA with the appropriate RIRs.

      iv. Ensure that up-to-date contact information is entered and maintained in the appropriate RIR databases.

   b. Identify the neighboring ASes with which the organization interconnects to exchange BGP routing information and/or IP data traffic.

      i. For each such network, identify the nature of the business relationship with the other AS (i.e., whether it an upstream transit service provider, a transit services customer, or a peering connection reflecting a settlement-free relationship).



   c. Document how the organization uses BGP routing by identifying:

      i. Which of the organization's own address prefixes originate from the organization's ASes using BGP announcements;

      ii. Which of the organization's address prefixes rely on the ASes of other organizations to originate their BGP announcements;

      iii. Which address prefixes held by other entities originate from the organization's networks using BGP announcements; and

      iv. Which processes (e.g., inter-domain traffic engineering) or services (e.g., DDoS mitigation services) might alter the origin AS or granularity (i.e., prefix length) of the organization's BGP announcements.

   d. Identify information systems and services internal to the organization that require Internet access and the corresponding address prefixes that are announced in BGP to enable that access. Assess the criticality (e.g., organizational mission impact) of maintaining resilient Internet routes for each address prefix originated from the organization's networks or originated on its behalf from other networks.

   e. Identify all contracted external/outsourced service providers (e.g., web, DNS, email, storage, etc.) critical to the organization's internal operations and document how routing to and from these services is provided. Assess the criticality of maintaining resilient Internet routes to the organization's external service providers.

   f. Establish, communicate, monitor, and maintain a risk management strategy, responsibilities, and policies for Internet routing. This may include evaluating the impact should the availability or integrity of BGP routing to the systems, services, and service providers identified above be disrupted.

   g. Based on the organization's cyber risk management strategy, identify address prefixes to prioritize for ROA creation and take action to do so.

      i. Consider prioritizing ROA creation for IP address blocks that contain the most critical services or have the most straightforward routing. In cases where ROA creation is prioritized for different address blocks, identify the specific criteria used for this decision process.

   h. Based on the risk management strategy, prioritize ASes for ROV coverage.

   i. Continue to monitor developments in BGP routing security, including best practice guidance for adopting new security mechanisms, threat analysis and incident reports, and new developments in standards and their commercialization. Factor any changes in this landscape into future risk management plan revisions.

Our part

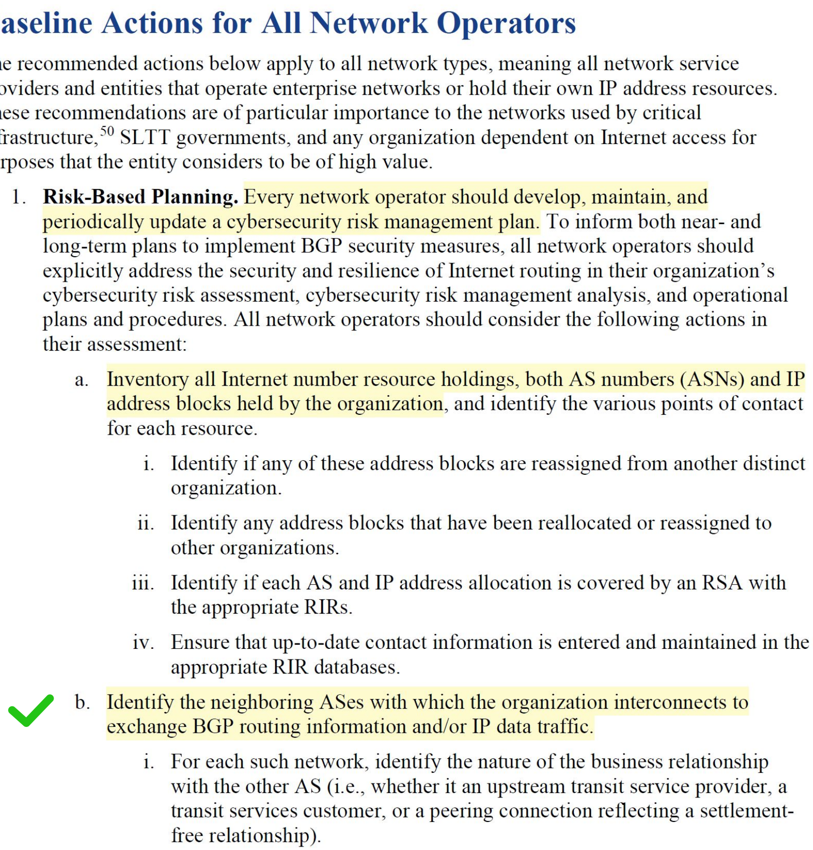
Let’s automate this Risk Assessment process…

…and bridge the gap between policy-based recommendations and actual network practice!

Let’s implement an open-source BGP-based Risk Assessment Toolbox!

🤞 this toolbox will drive a series of studies, each exploring different aspects of BGP security

Our implementation so far: on paper



Baseline Actions for All Network Operators

The recommended actions below apply to all network types, meaning all network service providers and entities that operate enterprise networks or hold their own IP address resources. These recommendations are of particular importance to the networks used by critical infrastructure,[50] SLTT governments, and any organization dependent on Internet access for purposes that the entity considers to be of high value.

1. **Risk-Based Planning.** Every network operator should develop, maintain, and periodically update a cybersecurity risk management plan. To inform both near- and long-term plans to implement BGP security measures, all network operators should explicitly address the security and resilience of Internet routing in their organization's cybersecurity risk assessment, cybersecurity risk management analysis, and operational plans and procedures. All network operators should consider the following actions in their assessment:

   a. Inventory all Internet number resource holdings, both AS numbers (ASNs) and IP address blocks held by the organization, and identify the various points of contact for each resource.

      i. Identify if any of these address blocks are reassigned from another distinct organization.

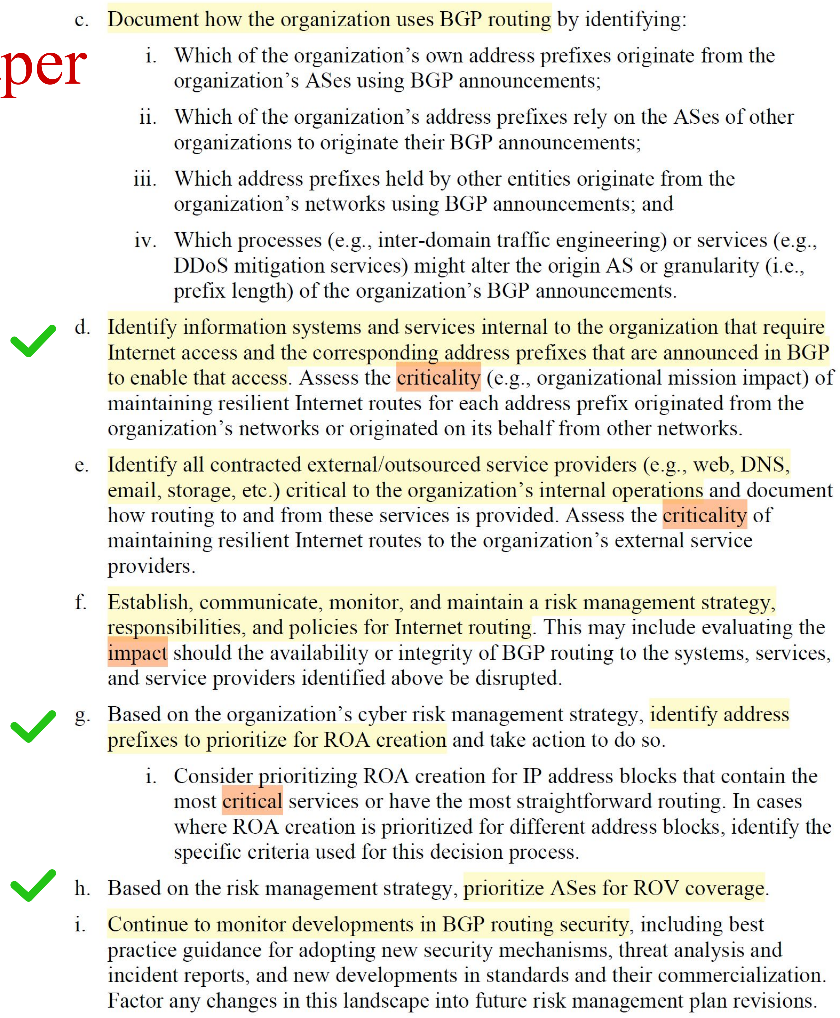
      ii. Identify any address blocks that have been reallocated or reassigned to other organizations.

      iii. Identify if each AS and IP address allocation is covered by an RSA with the appropriate RIRs.

      iv. Ensure that up-to-date contact information is entered and maintained in the appropriate RIR databases.

   ✓ b. Identify the neighboring ASes with which the organization interconnects to exchange BGP routing information and/or IP data traffic.

      i. For each such network, identify the nature of the business relationship with the other AS (i.e., whether it an upstream transit service provider, a transit services customer, or a peering connection reflecting a settlement-free relationship).



   c. Document how the organization uses BGP routing by identifying:

      i. Which of the organization's own address prefixes originate from the organization's ASes using BGP announcements;

      ii. Which of the organization's address prefixes rely on the ASes of other organizations to originate their BGP announcements;

      iii. Which address prefixes held by other entities originate from the organization's networks using BGP announcements; and

      iv. Which processes (e.g., inter-domain traffic engineering) or services (e.g., DDoS mitigation services) might alter the origin AS or granularity (i.e., prefix length) of the organization's BGP announcements.

   ✓ d. Identify information systems and services internal to the organization that require Internet access and the corresponding address prefixes that are announced in BGP to enable that access. Assess the criticality (e.g., organizational mission impact) of maintaining resilient Internet routes for each address prefix originated from the organization's networks or originated on its behalf from other networks.

   e. Identify all contracted external/outsourced service providers (e.g., web, DNS, email, storage, etc.) critical to the organization's internal operations and document how routing to and from these services is provided. Assess the criticality of maintaining resilient Internet routes to the organization's external service providers.

   f. Establish, communicate, monitor, and maintain a risk management strategy, responsibilities, and policies for Internet routing. This may include evaluating the impact should the availability or integrity of BGP routing to the systems, services, and service providers identified above be disrupted.

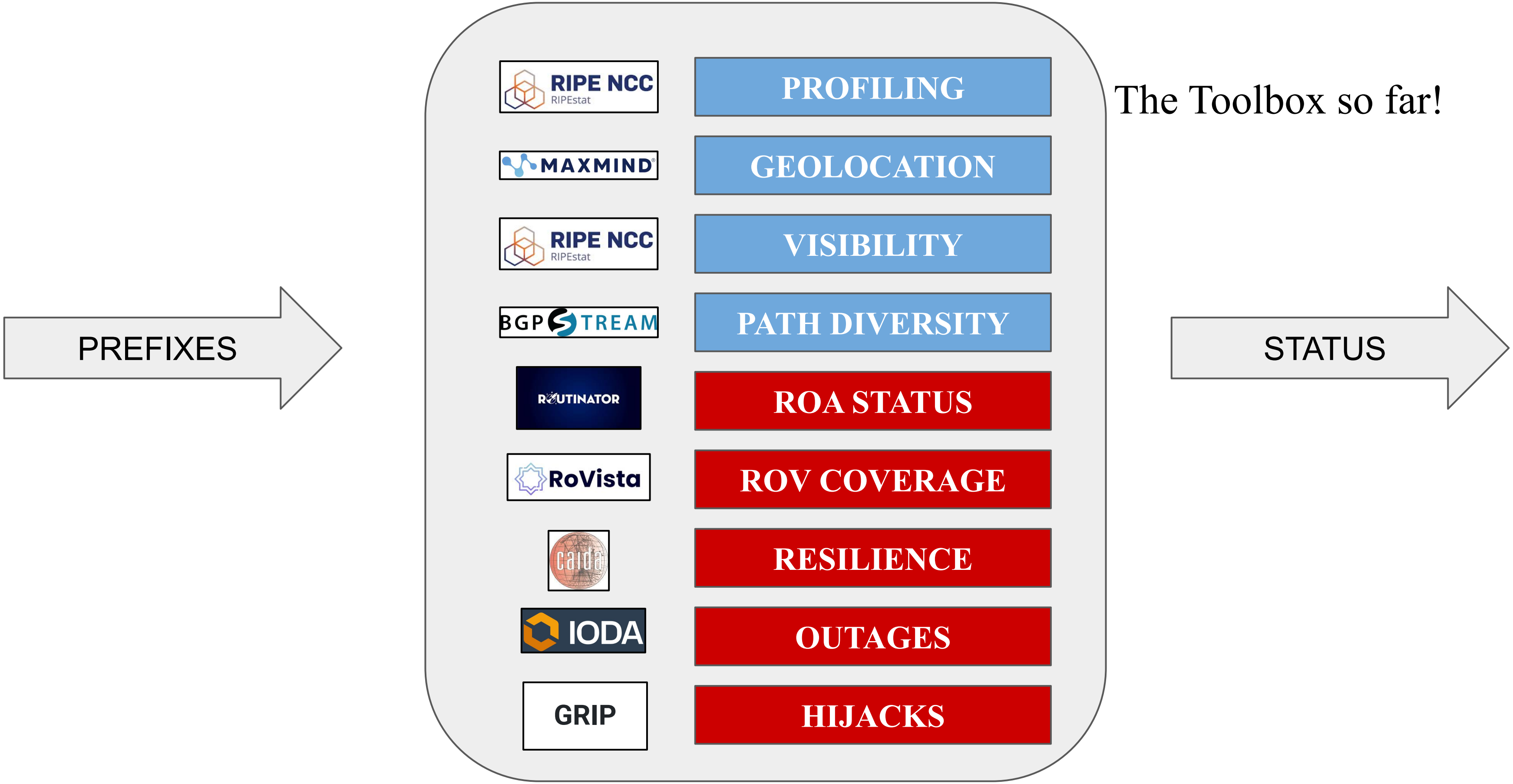
   ✓ g. Based on the organization's cyber risk management strategy, identify address prefixes to prioritize for ROA creation and take action to do so.

      i. Consider prioritizing ROA creation for IP address blocks that contain the most critical services or have the most straightforward routing. In cases where ROA creation is prioritized for different address blocks, identify the specific criteria used for this decision process.

   ✓ h. Based on the risk management strategy, prioritize ASes for ROV coverage.

   i. Continue to monitor developments in BGP routing security, including best practice guidance for adopting new security mechanisms, threat analysis and incident reports, and new developments in standards and their commercialization. Factor any changes in this landscape into future risk management plan revisions.

A Measurement-based Approach



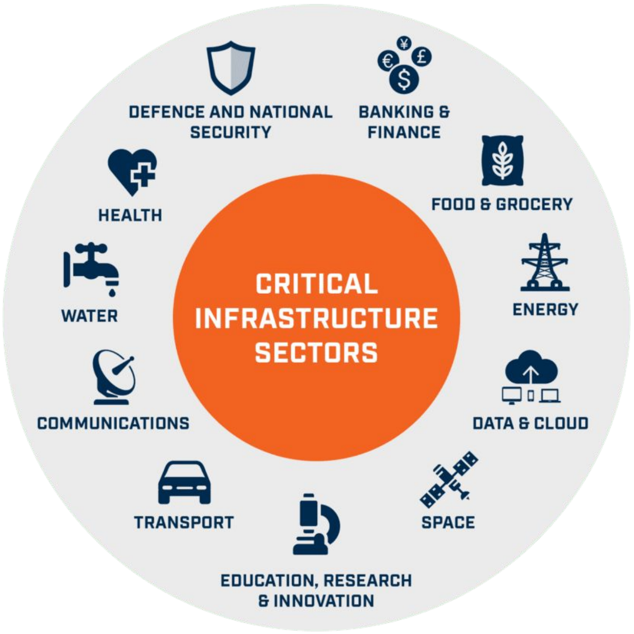
The Toolbox so far!

PREFIXES

RIPE NCC RIPEstat	PROFILING
MAXMIND	GEOLOCATION
RIPE NCC RIPEstat	VISIBILITY
BGPSTREAM	PATH DIVERSITY
ROUTINATOR	ROA STATUS
RoVista	ROV COVERAGE
caida	RESILIENCE
IODA	OUTAGES
GRIP	HIJACKS

STATUS

Input Selection: EU Critical Infrastructure Sectors



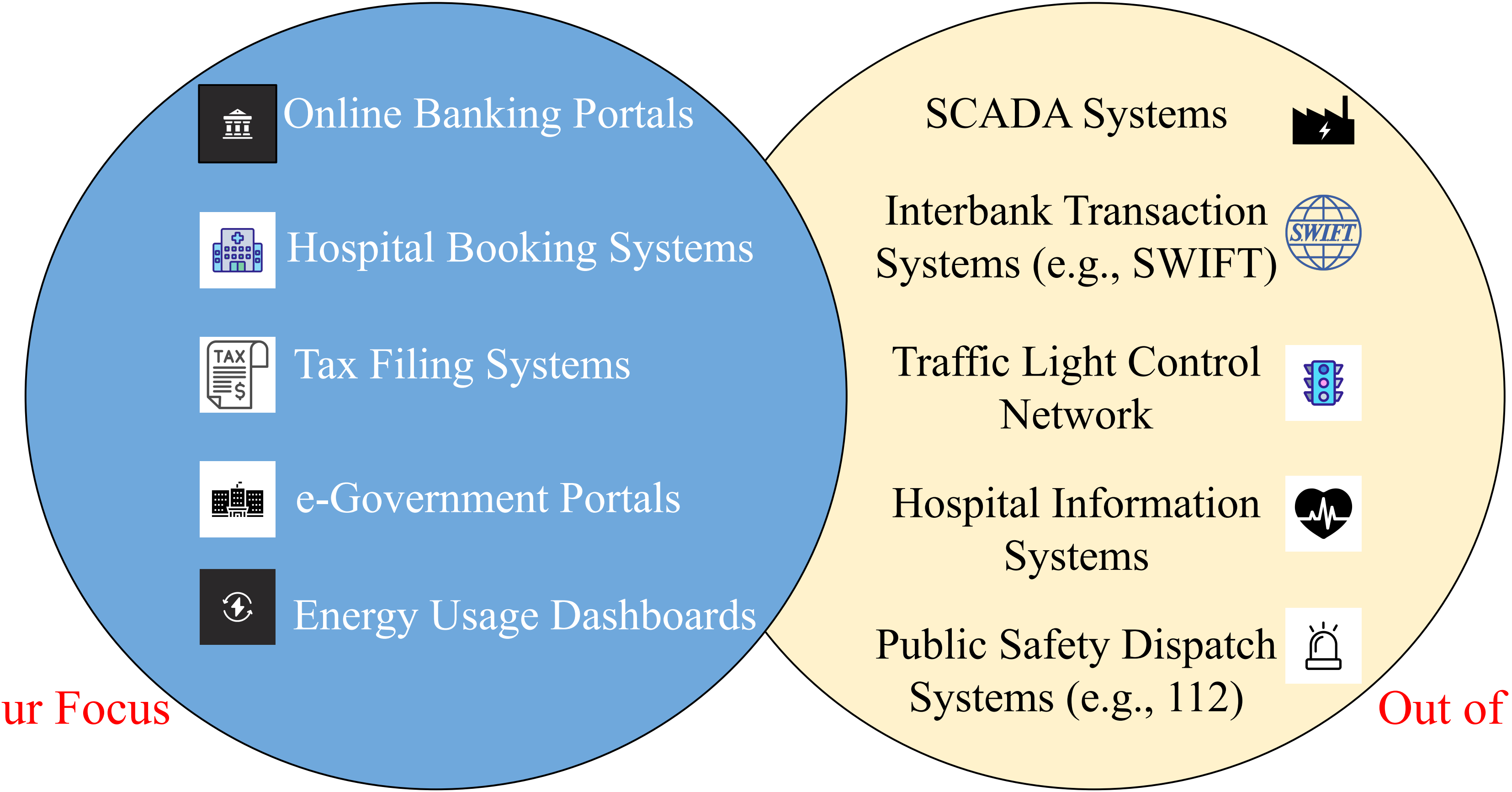
CRITICAL INFRASTRUCTURE SECTORS
DEFENCE AND NATIONAL SECURITY
BANKING & FINANCE
FOOD & GROCERY
ENERGY
DATA & CLOUD
SPACE
EDUCATION, RESEARCH & INNOVATION
TRANSPORT
COMMUNICATIONS
WATER
HEALTH

➔ To evaluate our approach, we apply our current toolbox to real-world datasets from ***Critical Infrastructure*** sectors.

➔ The term ***Critical Infrastructure*** sectors (as recognized by governments and policymakers) refers to ***essential systems whose disruption would significantly impact public health, safety, and economic stability.***

➔ Failures or attacks on underlying systems (such as BGP or DNS) could ***cripple*** critical online services/domains, disrupt communication, and ***impact*** essential operations worldwide.

Scope: Internet-facing part vs Core Infrastructure



Online Banking Portals

Hospital Booking Systems

Tax Filing Systems

e-Government Portals

Energy Usage Dashboards

SCADA Systems

Interbank Transaction Systems (e.g., SWIFT)

Traffic Light Control Network

Hospital Information Systems

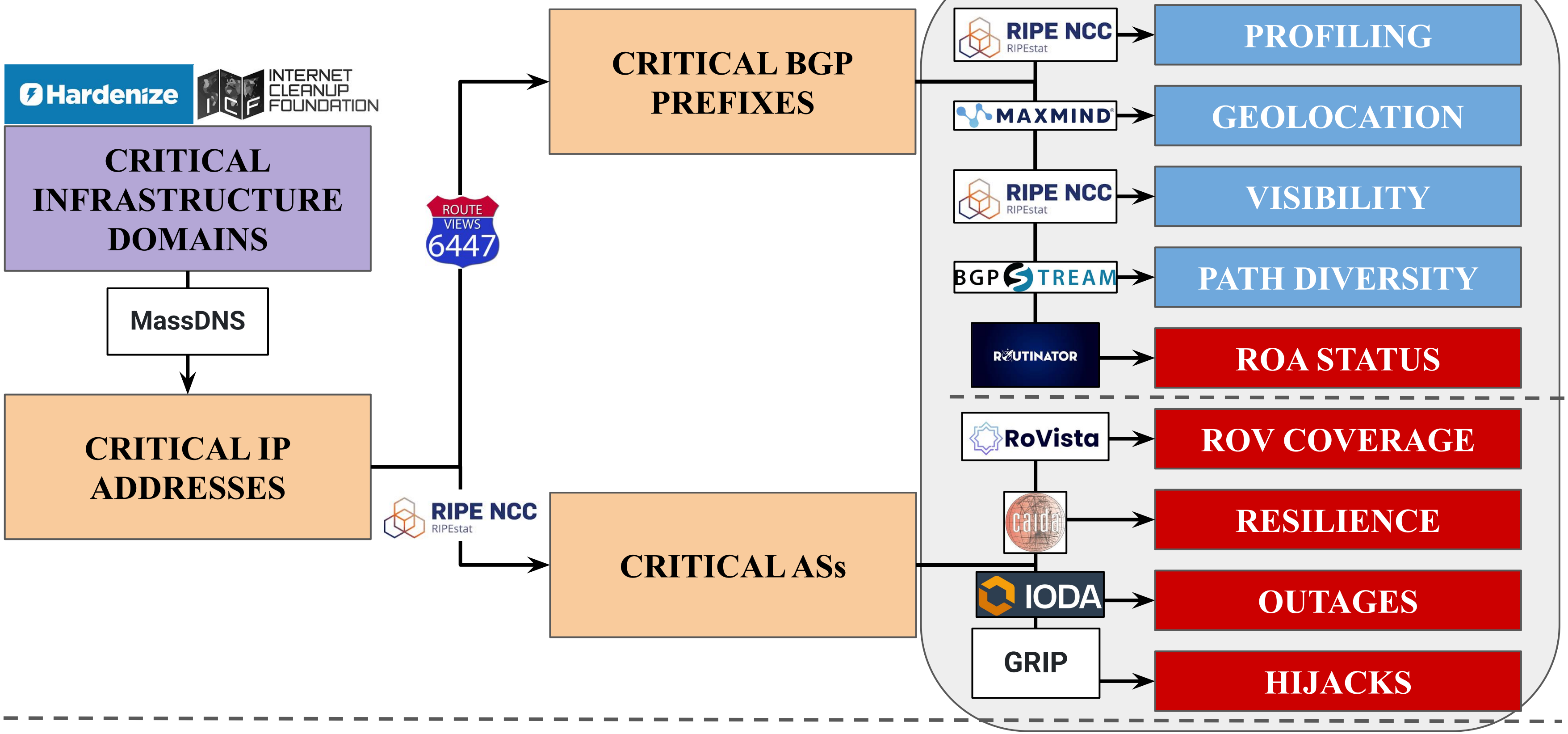
Public Safety Dispatch Systems (e.g., 112)

Our Focus

Out of Scope

A Measurement-based Approach

The Toolbox so far!



CRITICAL INFRASTRUCTURE DOMAINS

MassDNS

CRITICAL IP ADDRESSES

CRITICAL BGP PREFIXES

CRITICAL ASs

PROFILING

GEOLOCATION

VISIBILITY

PATH DIVERSITY

ROA STATUS

ROV COVERAGE

RESILIENCE

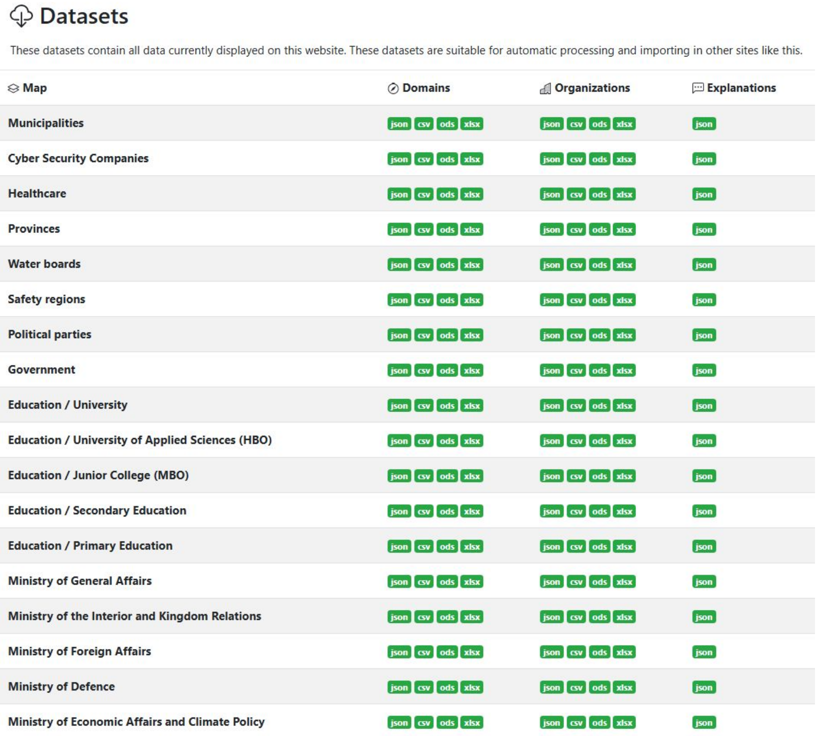
OUTAGES

HIJACKS

GRIP

INPUT	OUTPUT	NETWORK ANALYSIS	SECURITY ANALYSIS

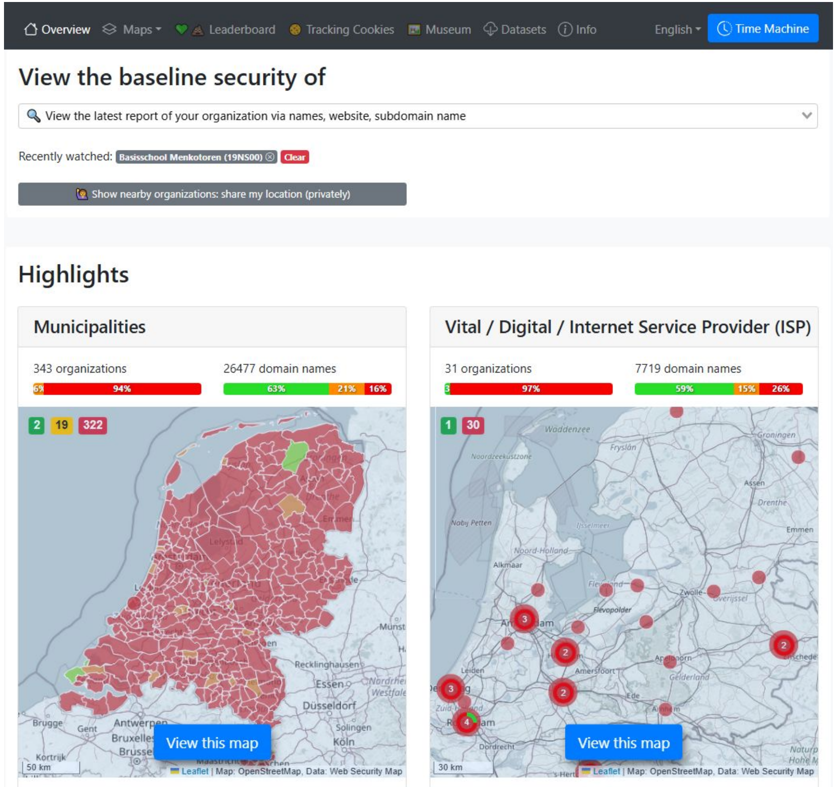
The input: basisbeveiliging.nl



Datasets

These datasets contain all data currently displayed on this website. These datasets are suitable for automatic processing and importing in other sites like this.

Map	Domains	Organizations	Explanations
Municipalities	json csv ods xlsx	json csv ods xlsx	json
Cyber Security Companies	json csv ods xlsx	json csv ods xlsx	json
Healthcare	json csv ods xlsx	json csv ods xlsx	json
Provinces	json csv ods xlsx	json csv ods xlsx	json
Water boards	json csv ods xlsx	json csv ods xlsx	json
Safety regions	json csv ods xlsx	json csv ods xlsx	json
Political parties	json csv ods xlsx	json csv ods xlsx	json
Government	json csv ods xlsx	json csv ods xlsx	json
Education / University	json csv ods xlsx	json csv ods xlsx	json
Education / University of Applied Sciences (HBO)	json csv ods xlsx	json csv ods xlsx	json
Education / Junior College (MBO)	json csv ods xlsx	json csv ods xlsx	json
Education / Secondary Education	json csv ods xlsx	json csv ods xlsx	json
Education / Primary Education	json csv ods xlsx	json csv ods xlsx	json
Ministry of General Affairs	json csv ods xlsx	json csv ods xlsx	json
Ministry of the Interior and Kingdom Relations	json csv ods xlsx	json csv ods xlsx	json
Ministry of Foreign Affairs	json csv ods xlsx	json csv ods xlsx	json
Ministry of Defence	json csv ods xlsx	json csv ods xlsx	json
Ministry of Economic Affairs and Climate Policy	json csv ods xlsx	json csv ods xlsx	json



View the baseline security of

View the latest report of your organization via names, website, subdomain name

Recently watched: Basisschool Menkotoren (19NS00) Clear

Show nearby organizations: share my location (privately)

Highlights

Municipalities

343 organizations — 6% 94%

26477 domain names — 63% 21% 16%

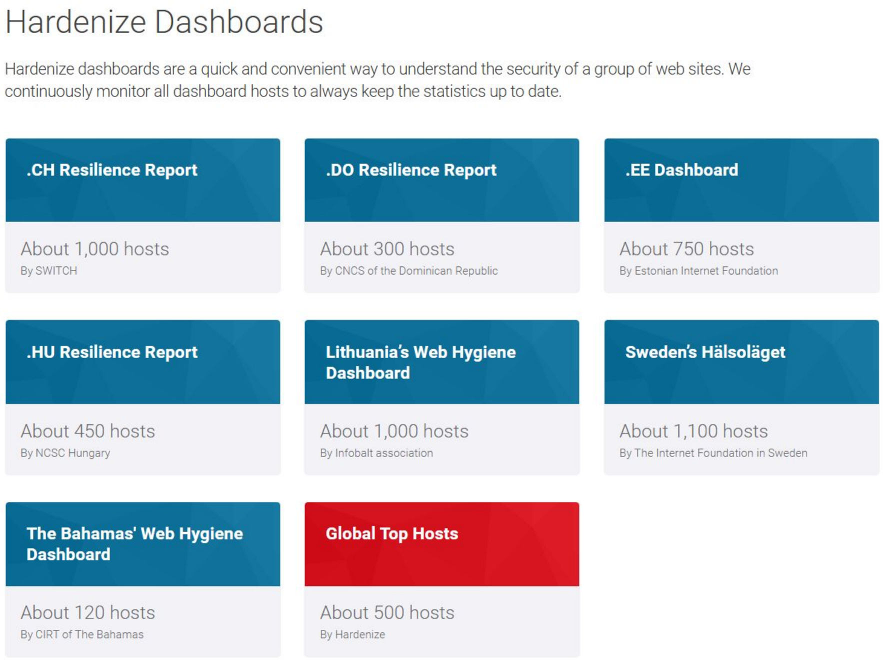
Vital / Digital / Internet Service Provider (ISP)

31 organizations — 3 97%

7719 domain names — 59% 15% 26%

❖ **Basisbeveiliging.nl** is an initiative by the **Internet Cleanup Foundation**, which assesses and publicly reports on the basic digital security of Dutch organizations across sectors like government, healthcare, and education.

The input: hardenize.com



Hardenize Dashboards

Hardenize dashboards are a quick and convenient way to understand the security of a group of web sites. We continuously monitor all dashboard hosts to always keep the statistics up to date.

.CH Resilience Report
About 1,000 hosts
By SWITCH

.DO Resilience Report
About 300 hosts
By CNCS of the Dominican Republic

.EE Dashboard
About 750 hosts
By Estonian Internet Foundation

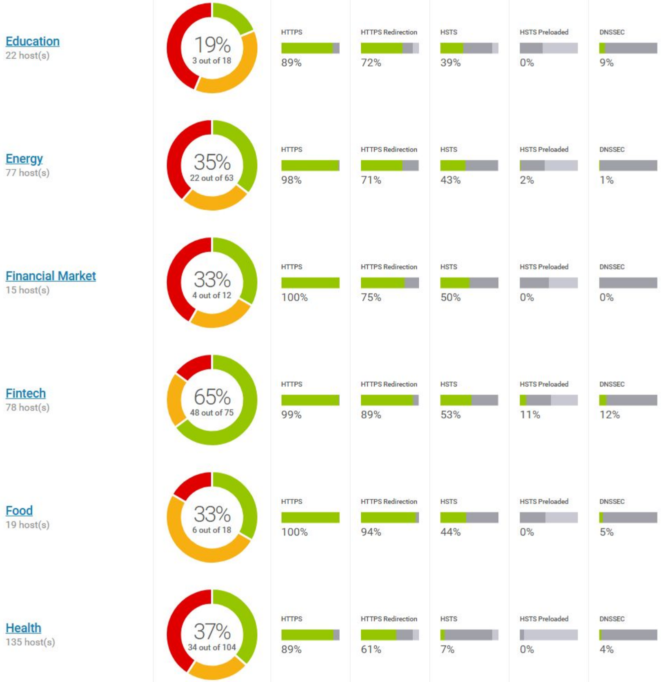
.HU Resilience Report
About 450 hosts
By NCSC Hungary

Lithuania's Web Hygiene Dashboard
About 1,000 hosts
By Infobalt association

Sweden's Hälsoläget
About 1,100 hosts
By The Internet Foundation in Sweden

The Bahamas' Web Hygiene Dashboard
About 120 hosts
By CIRT of The Bahamas

Global Top Hosts
About 500 hosts
By Hardenize



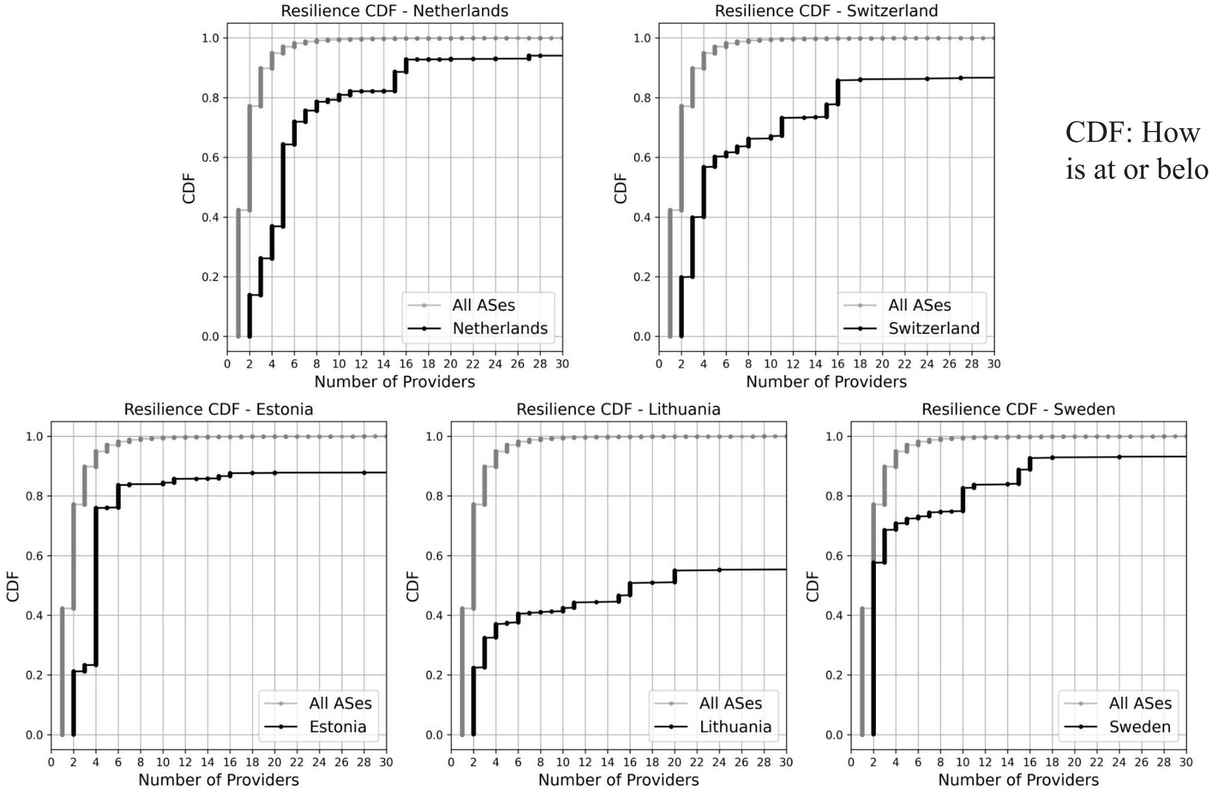
		HTTPS	HTTPS Redirection	HSTS	HSTS Preloaded	DNSSEC
Education 22 host(s)	19% 3 out of 18	89%	72%	39%	0%	9%
Energy 77 host(s)	35% 22 out of 63	98%	71%	43%	2%	1%
Financial Market 15 host(s)	33% 4 out of 12	100%	75%	50%	0%	0%
Fintech 78 host(s)	65% 48 out of 75	99%	89%	53%	11%	12%
Food 19 host(s)	33% 6 out of 18	100%	94%	44%	0%	5%
Health 135 host(s)	37% 34 out of 104	89%	61%	7%	0%	4%

- **Hardenize.com** offers comprehensive assessments and public reports of security configurations, enabling organizations across multiple countries (i.e., CH, EE, LT, SE) to monitor and improve their digital infrastructure.

✅the toolbox… ✅the approach… ✅the data..

Time for Results!

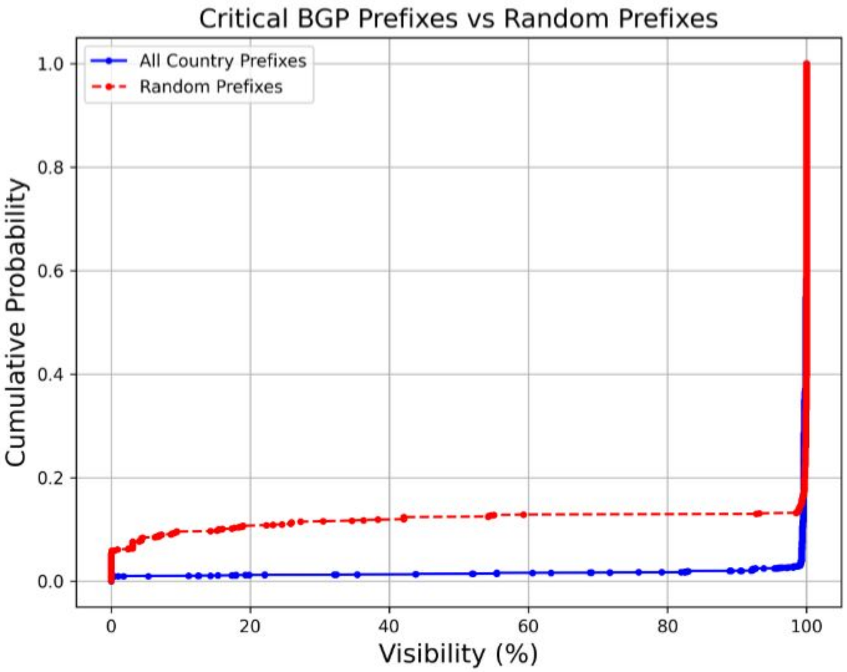
Multi-homing adoption of *Critical ASes*



CDF: How much of the data (y-axis) is at or below an x-axis point?

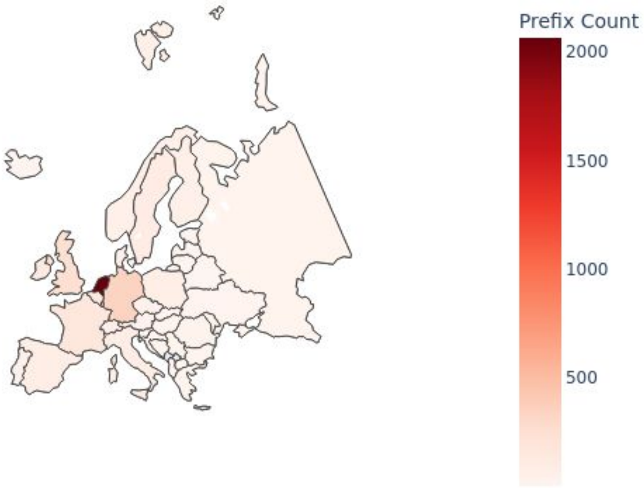
★ *Critical ASes* are **resilient** in terms of multihoming, since, not a single AS relies only on a single upstream provider. Single-homed ASes are SPOF!

Visibility *Critical BGP Prefixes*

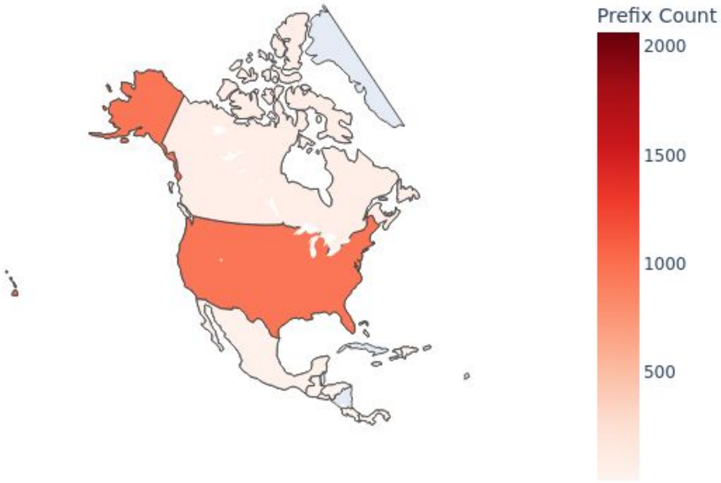


★ Constant monitoring is important: Low visibility could indicate that a prefix may become unreachable or lead to service degradation.

Jurisdictional Dependencies of *Critical BGP Prefixes*



Netherlands - Europe Map

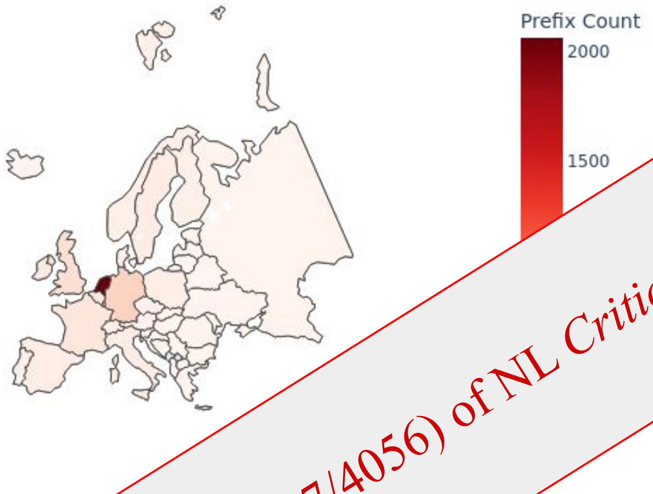


Netherlands - US Map

★ *Critical BGP Prefixes* have a strong presence in the country of origin and the US.

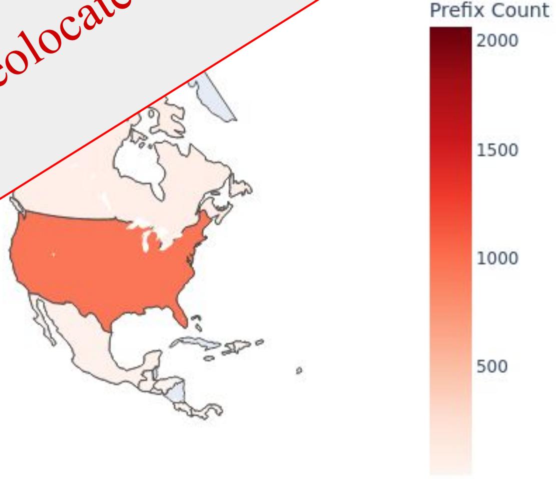
★ The heavy US concentration suggests that disruptions in US-based networks (or political-regulatory shifts) can potentially propagate globally.

Jurisdictional Dependencies of *Critical BGP Pr*



Neth

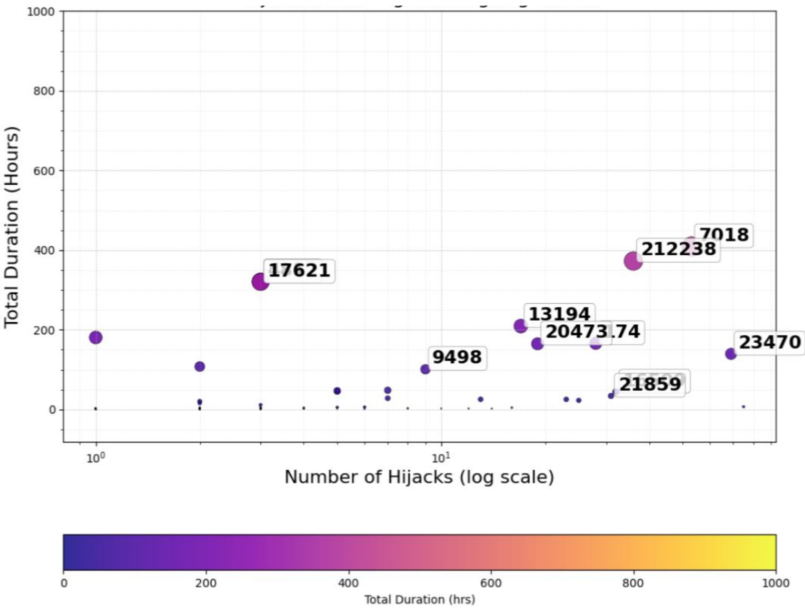
~25% (957/4056) of NL *Critical BGP Prefixes* geolocate in the US!

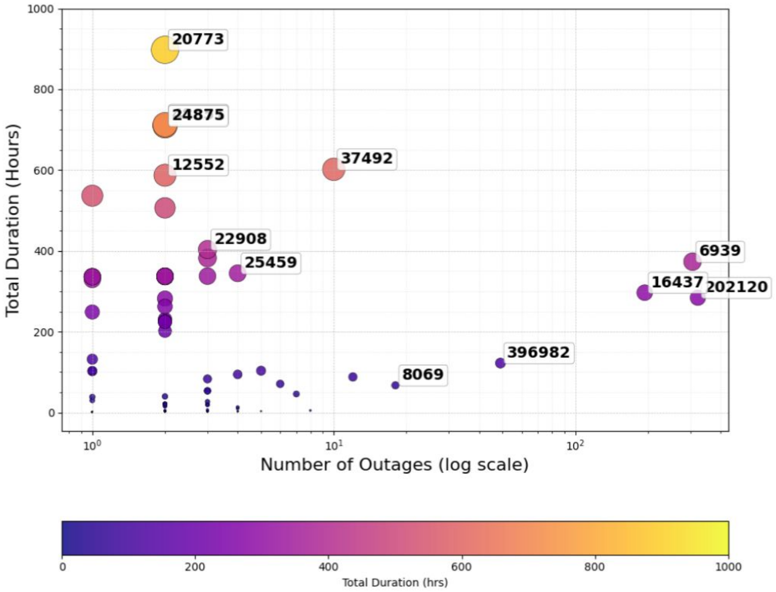


Netherlands - US Map

- ★ *Critical BG* *es* have a strong presence in the country of origin and the US.
- ★ The heavy US concentration suggests that disruptions in US-based networks (or political-regulatory shifts) can potentially propagate globally.

Anomalies in Critical ASes





★ Some Critical ASes suffer from **frequent or prolonged network outages**, highlighting operational instability or lack of redundancy in CI infrastructure.

★ **Large ASes (ATT, Cogent, Amazon)** experience **numerous BGP hijacks**, showing that even well-resourced networks remain vulnerable to routing attacks.

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

★ …more than 40% of Critical ASes fail to perform RoV, which undermines overall RPKI!

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

★ …more than 40% of Critical ASes fail to perform RoV, which undermines overall RPKI!

★ NetOps should prioritize RoA signing of *Critical Prefixes* and RoV enforcement.

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

★ …more than 40% of Critical ASes fail to perform RoV, which undermines overall RPKI!

★ NetOps should prioritize RoA signing of *Critical Prefixes* and RoV enforcement.

★ Policy-makers (e.g., FCC, ENISA, ICANN) should incentivize RPKI compliance:

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

★ …more than 40% of Critical ASes fail to perform RoV, which undermines overall RPKI!

★ NetOps should prioritize RoA signing of *Critical Prefixes* and RoV enforcement.

★ Policy-makers (e.g., FCC, ENISA, ICANN) should incentivize RPKI compliance:

○ Tax benefits

Resource Public Key Infrastructure (RPKI)

Route Origin Authorization (RoA)
A cryptographic statement that declares which AS is authorized to announce a specific IP prefix.

Route Origin Validation (RoV)
A router-side mechanism that checks BGP announcements against RoAs enabling networks to **filter out unauthorized/invalid routes**.

RPKI = RoA + RoV

★ Even though, EU *Critical BGP Prefixes* demonstrate a good RoA compliance rate (67% for Sweden and more than 80% for the rest of the countries)....

★ …more than 40% of Critical ASes fail to perform RoV, which undermines overall RPKI!

★ NetOps should prioritize RoA signing of *Critical Prefixes* and RoV enforcement.

★ Policy-makers (e.g., FCC, ENISA, ICANN) should incentivize RPKI compliance:

  ○ Tax benefits

  ○ Grants to smaller ISPs

Take-away Message

★ We aim to bridge the gap between policy-based recommendations and actual network practice. To that end, we design and implement a *BGP-based Risk Assessment Toolbox*.

Contact Info: s.kastanakis@utwente.nl Personal Website: https://kastanakis.github.io/cv/

Take-away Message

★ We aim to bridge the gap between policy-based recommendations and actual network practice. To that end, we design and implement a *BGP-based Risk Assessment Toolbox*.

★ Using our toolbox, we investigate the network and security postures of *Critical BGP Prefixes* across 5 EU countries. Two important insights derived are:

Contact Info: s.kastanakis@utwente.nl Personal Website: https://kastanakis.github.io/cv/

Take-away Message

- ★ We aim to bridge the gap between policy-based recommendations and actual network practice. To that end, we design and implement a *BGP-based Risk Assessment Toolbox*.

- ★ Using our toolbox, we investigate the network and security postures of *Critical BGP Prefixes* across 5 EU countries. Two important insights derived are:
  - ○ *Critical BGP Prefixes* exhibit a heavy concentration in the country of origin and the US, which suggests that disruptions (or political-regulatory shifts) in US-based networks can potentially propagate globally.

Contact Info: s.kastanakis@utwente.nl Personal Website: https://kastanakis.github.io/cv/

Take-away Message

- ★ We aim to bridge the gap between policy-based recommendations and actual network practice. To that end, we design and implement a *BGP-based Risk Assessment Toolbox*.

- ★ Using our toolbox, we investigate the network and security postures of *Critical BGP Prefixes* across 5 EU countries. Two important insights derived are:
    - ○ *Critical BGP Prefixes* exhibit a heavy concentration in the country of origin and the US, which suggests that disruptions (or political-regulatory shifts) in US-based networks can potentially propagate globally.
    - ○ *Critical ASes* demonstrate high RoA compliance but low RoV enforcement undermining the overall RPKI security.

Contact Info: s.kastanakis@utwente.nl Personal Website: https://kastanakis.github.io/cv/

Take-away Message

★ We aim to bridge the gap between policy-based recommendations and actual network practice. To that end, we design and implement a *BGP-based Risk Assessment Toolbox*.

★ Using our toolbox, we investigate the network and security postures of *Critical BGP Prefixes* across 5 EU countries. Two important insights derived are:

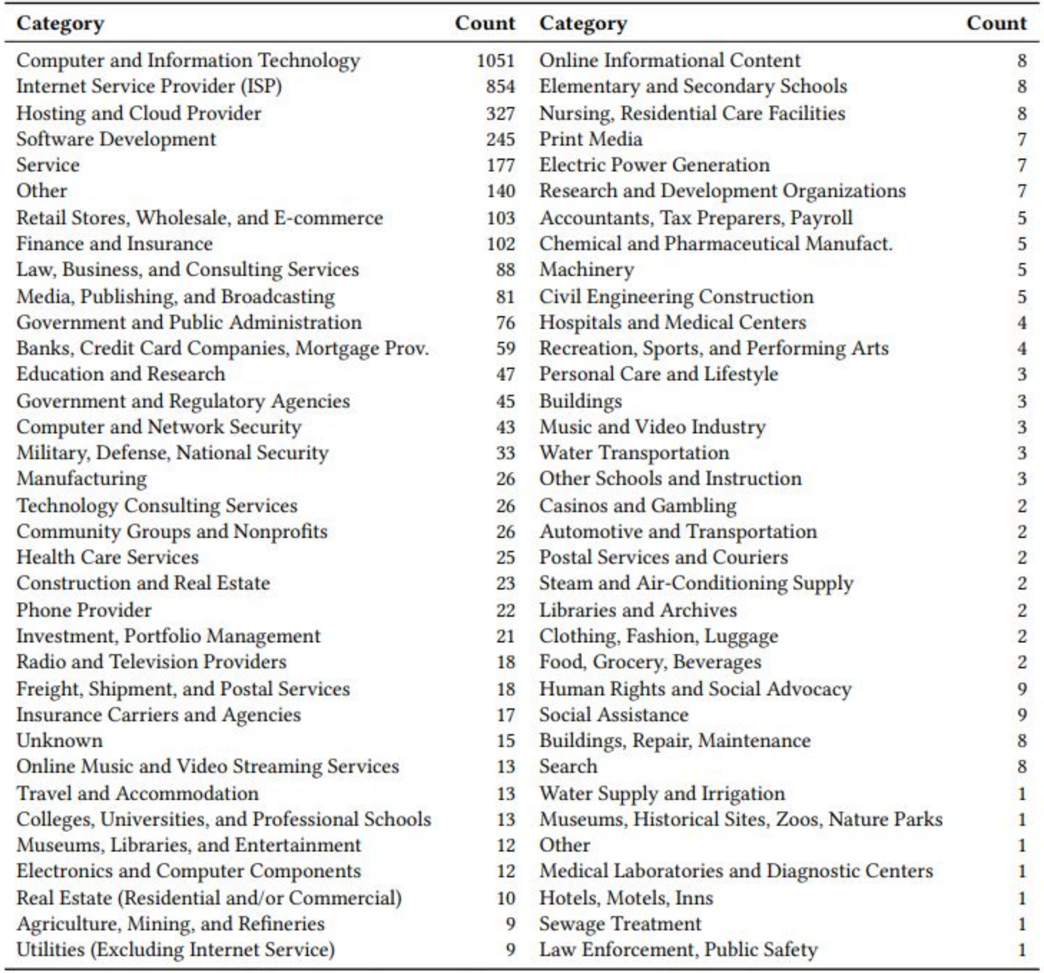
- ○ *Critical BGP Prefixes* exhibit a heavy concentration in the country of origin and the US, which suggests that disruptions (or political-regulatory shifts) in US-based networks can potentially propagate globally.
- ○ *Critical ASes* demonstrate high RoA compliance but low RoV enforcement undermining the overall RPKI security.

★ Netops can use such a tool to: i) prioritize RoA of *Critical BGP Prefixes*, ii) filter low-RoV enforcing ASes, or iii) favor certain AS paths based on the intermediate RoV scores.

Contact Info: s.kastanakis@utwente.nl Personal Website: https://kastanakis.github.io/cv/

Backup Slides

AS2Type



Category	Count	Category	Count
Computer and Information Technology	1051	Online Informational Content	8
Internet Service Provider (ISP)	854	Elementary and Secondary Schools	8
Hosting and Cloud Provider	327	Nursing, Residential Care Facilities	8
Software Development	245	Print Media	7
Service	177	Electric Power Generation	7
Other	140	Research and Development Organizations	7
Retail Stores, Wholesale, and E-commerce	103	Accountants, Tax Preparers, Payroll	5
Finance and Insurance	102	Chemical and Pharmaceutical Manufact.	5
Law, Business, and Consulting Services	88	Machinery	5
Media, Publishing, and Broadcasting	81	Civil Engineering Construction	5
Government and Public Administration	76	Hospitals and Medical Centers	4
Banks, Credit Card Companies, Mortgage Prov.	59	Recreation, Sports, and Performing Arts	4
Education and Research	47	Personal Care and Lifestyle	3
Government and Regulatory Agencies	45	Buildings	3
Computer and Network Security	43	Music and Video Industry	3
Military, Defense, National Security	33	Water Transportation	3
Manufacturing	26	Other Schools and Instruction	3
Technology Consulting Services	26	Casinos and Gambling	2
Community Groups and Nonprofits	26	Automotive and Transportation	2
Health Care Services	25	Postal Services and Couriers	2
Construction and Real Estate	23	Steam and Air-Conditioning Supply	2
Phone Provider	22	Libraries and Archives	2
Investment, Portfolio Management	21	Clothing, Fashion, Luggage	2
Radio and Television Providers	18	Food, Grocery, Beverages	2
Freight, Shipment, and Postal Services	18	Human Rights and Social Advocacy	9
Insurance Carriers and Agencies	17	Social Assistance	9
Unknown	15	Buildings, Repair, Maintenance	8
Online Music and Video Streaming Services	13	Search	8
Travel and Accommodation	13	Water Supply and Irrigation	1
Colleges, Universities, and Professional Schools	13	Museums, Historical Sites, Zoos, Nature Parks	1
Museums, Libraries, and Entertainment	12	Other	1
Electronics and Computer Components	12	Medical Laboratories and Diagnostic Centers	1
Real Estate (Residential and/or Commercial)	10	Hotels, Motels, Inns	1
Agriculture, Mining, and Refineries	9	Sewage Treatment	1
Utilities (Excluding Internet Service)	9	Law Enforcement, Public Safety	1

The input: why is this suitable for our analysis?

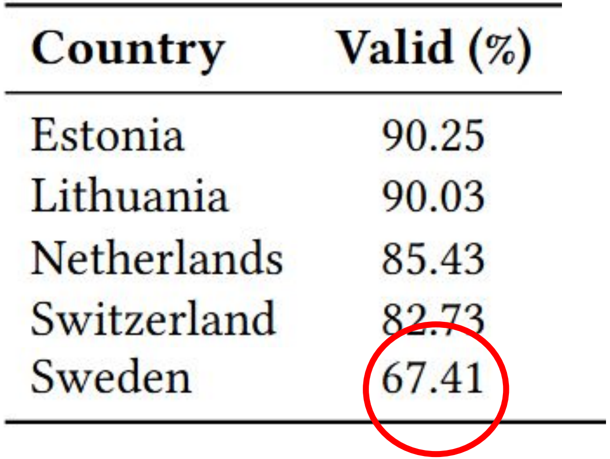
Hardenize INTERNET CLEANUP FOUNDATION

🎯 **Sector-Focused**
Both platforms mainly assess organizations in **critical sectors** (e.g., government, healthcare, education, and finance) aligning directly with the scope of this study.

🌍 **Geographically Relevant**
These tools offer **region-specific datasets** (e.g., Netherlands, Sweden, Estonia, Switzerland), which supports our focus on **European services** and jurisdictionally scoped analysis.

🔎 **Security-Oriented and Publicly Available**
Their datasets reflect **actively monitored, real-world services** with known security profiles. This makes them ideal for infrastructure measurement through DNS and BGP mapping.

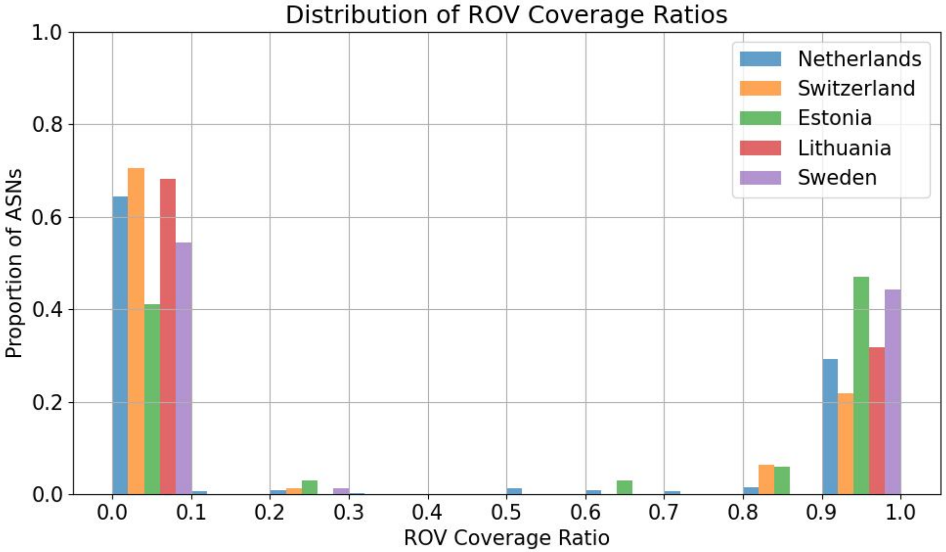
RoA Status of *Critical BGP Prefixes*



Country	Valid (%)
Estonia	90.25
Lithuania	90.03
Netherlands	85.43
Switzerland	82.73
Sweden	67.41

- ★ NetOps should prioritize signing of no-RoA *Critical BGP Prefixes*!
- ★ Policy-makers (e.g., FCC, ENISA, ICANN) should incentivize RPKI compliance:
  - ○ Tax benefits
  - ○ Grants to smaller ISPs

RoV Status of *Critical ASes*

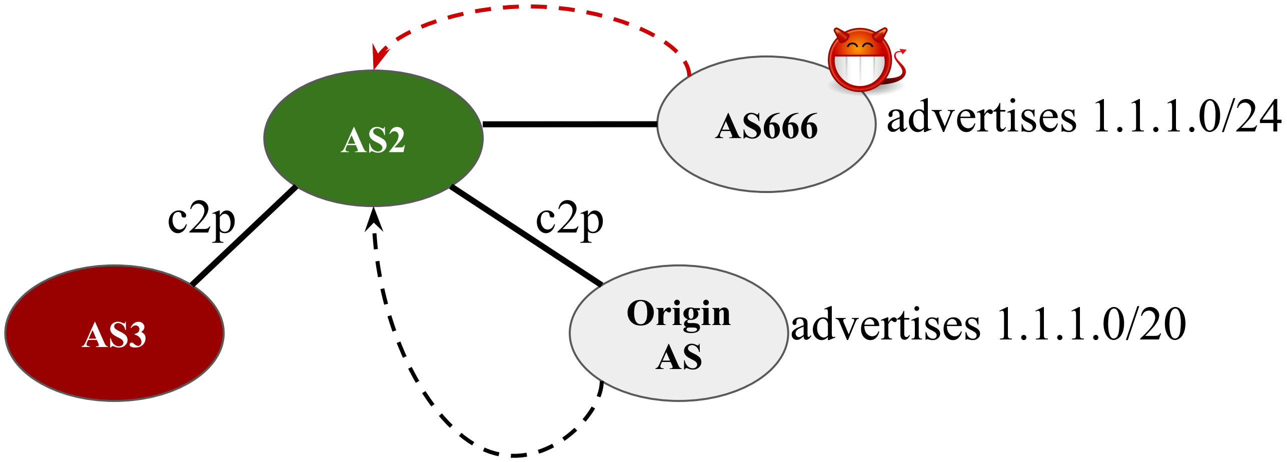


★ Without RoV, invalid routes remain unfiltered and undermine the effectiveness of RPKI.

★ Netops could prioritize AS paths on their routing tables based on the individual RoV scores of intermediate ASes in the path!

Collateral Impact: Measuring Indirect RPKI Protection

★ Collateral Impact suggests that even if an AS doesn’t implement RoV, it can still be protected by upstream ASes which filter invalid routes!



Example: AS3 doesn’t fall victim of AS666, since, AS2 implements RoV

🟥 – – ➤ Malicious Announcement

🟩 – – ➤ Benign Announcement

Collateral Impact: Measuring Indirect RPKI Protection

- ★ Collateral Impact suggests that even if an AS doesn’t implement RoV, it can still be protected by upstream ASes which filter invalid routes!

- ★ **Filtering can only propagate in one direction**: A provider can protect its customers (c2p), but a customer cannot protect its provider (p2c), nor can peers protect peers (p2p).

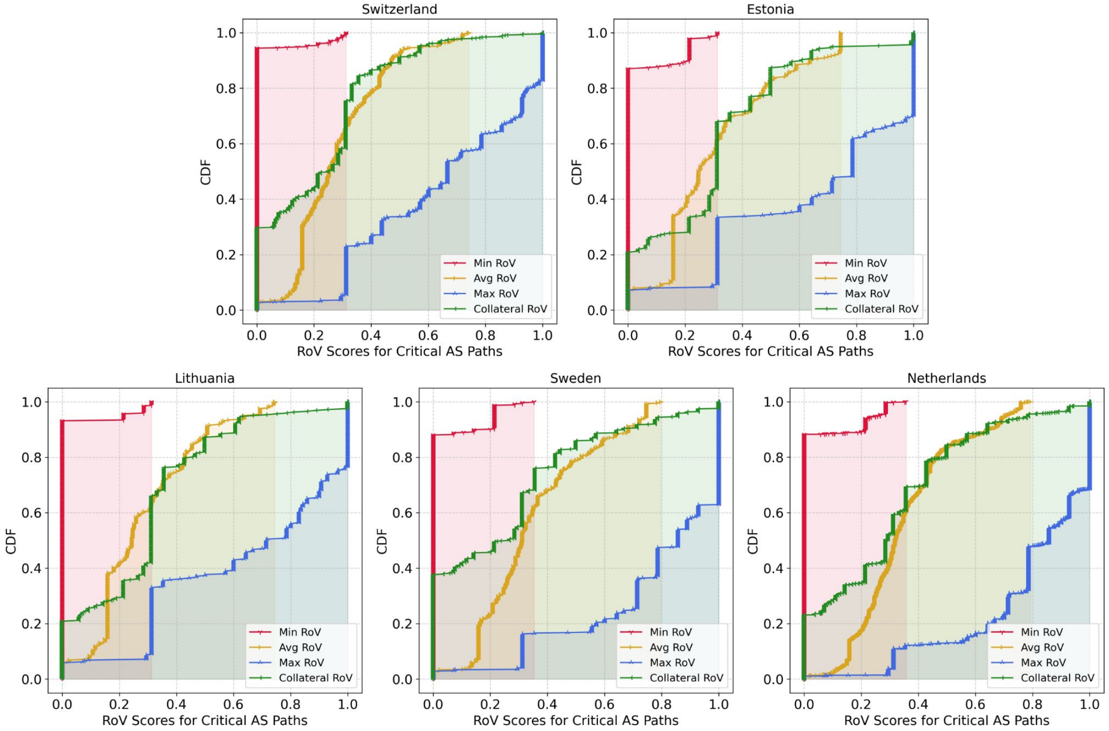
- ★ How we measure it:
  - ○ We target only *Critical Prefixes* with valid RoAs (since RoV wouldnt make sense)
  - ○ We walk the *Critical AS path* hop-by-hop
  - ○ For each c2p link we identify, we update the overall path score with the individual RoV score of the provider

Collateral Impact of RoV deployment

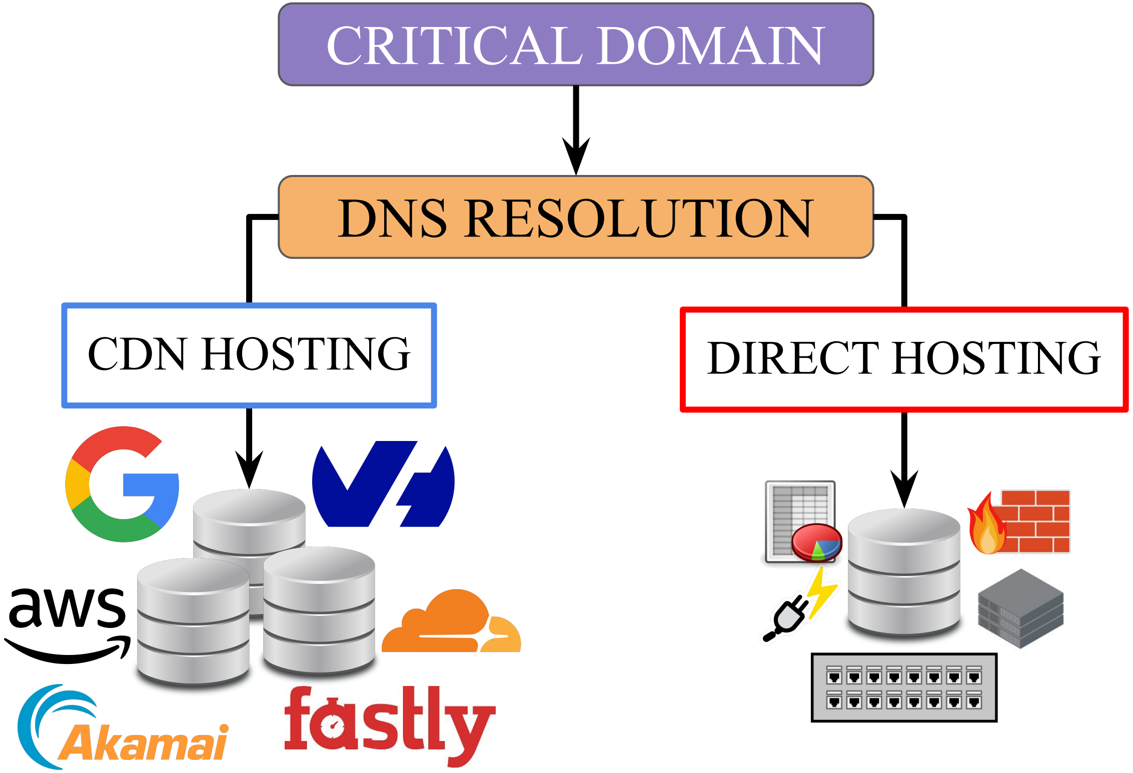
★ Many *Critical AS paths* have low RoV scores, with minimum values near zero, making them **vulnerable to hijacks**.

★ Average and maximum RoV scores **vary across countries**, showing partial but inconsistent adoption of RPKI validation.

★ Collateral RoV suggests that **paths benefit from** neighboring ASes with **stronger RoV practices**.



Future Work: Differentiate between CDN vs non-CDN hosted domains


CRITICAL DOMAIN
DNS RESOLUTION
CDN HOSTING
DIRECT HOSTING
aws
Akamai
fastly