Critical BGP Prefixes: A Measurement-based Investigation of Critical Infrastructure Security

Savvas Kastanakis*, Shyam Krishna Khadka*, Ebrima Jaw*, Cristian Hesselman*‡
*University of Twente, Netherlands ‡SURF, Netherlands
Emails: {s.kastanakis, s.k.khadka, e.jaw, c.e.w.hesselman}@utwente.nl

***Abstract*—*Critical Infrastructure (CI)* sectors, such as energy, finance, healthcare, and public administration, rely heavily on the Internet to deliver essential services, yet their resilience increasingly depends on the security of the global routing system. This paper presents the first large-scale, measurement-driven study to identify and analyze *Critical BGP Prefixes*, defined as the Internet address blocks that host publicly reachable *CI* services in Europe. Using a domain name–based mapping methodology, aligned with formal EU definitions of *CI* sectors, we systematically associate thousands of government- and industry-owned domains across five European countries (Netherlands, Switzerland, Sweden, Lithuania, and Estonia) with their underlying BGP prefixes and origin Autonomous Systems (ASes).**

We characterize these *Critical BGP Prefixes* and *Critical ASes* across multiple dimensions, including network structure, jurisdictional dependencies, and routing security posture. Our analysis reveals a high degree of centralization, with a small number of ASes and cloud providers supporting a disproportionate share of *CI* services. Finally, we observe persistent exposure to BGP hijacks and foreign infrastructure dependencies (particularly reliance on U.S.-based networks), which challenge the European digital sovereignty.

We publicly release our methodology and datasets to promote transparency and reproducibility, offering a data-driven framework for policymakers and network operators to strengthen the resilience and autonomy of Europe's digital backbone.

I. Introduction

Formally, *Critical Infrastructure (CI)* refers to the essential systems and networks whose incapacitation or destruction would result in significant disruptions to public health, safety and economic stability [1]. These systems span vital sectors such as energy, healthcare, finance, and information technology. Their resilience ensures the continuity of essential services, even in the face of natural disasters, cyber threats, or other emergent challenges. However, the security of these systems is increasingly threatened by systemic vulnerabilities in the underlying Border Gateway Protocol (BGP), which they rely on [2], [3].

BGP [4] is the routing protocol that exchanges network reachability information between Autonomous Systems (ASes) on the Internet, with prefixes representing the specific blocks of IP addresses that BGP advertises and routes. Since its inception, BGP lacks basic authentication and integrity mechanisms, making it easy for malicious actors to manipulate traffic, intercept sensitive data, cut off entire networks or even impersonate critical services [5].

Amid these growing threats, there remains a significant gap in systematically understanding which BGP prefixes underpin *CI* services. Without this clarity, all prefixes risk being treated equally, even though the impact of a hijack on a generic web hosting service is incomparable to that of an attack on emergency response networks, government agencies, financial institutions, or power grids.

To bridge this gap, we introduce the concept of *Critical BGP Prefixes*, which we define as *IP address ranges associated with CI's publicly visible services*. In this study, we restrict our scope to Europe, guided by European definitions of *CI* [1] and analyze prefixes across five countries: the Netherlands, Switzerland, Sweden, Lithuania, and Estonia. Within this regional context, we investigate three fundamental questions: RQ1) *Which Internet-facing BGP prefixes underpin European Critical Infrastructure services?* RQ2) *What are the network and security characteristics of European Critical BGP Prefixes?* RQ3) *To what extent do European Critical BGP Prefixes depend on non-European infrastructure, and what are the implications for resilience and digital sovereignty?*

Importantly, our analysis targets the Internet-facing layer of *CI*, encompassing websites, DNS servers, public APIs, and other external network services. We exclude internal operational systems such as energy grids or private interbank networks, which are not directly observable through Internet measurement. Specifically, our contributions are as follows:

1) We introduce a domain name–based methodology to infer *Critical BGP Prefixes* and their originating *Critical ASes*, aligning with formal EU definitions of *CI* sectors.
2) We investigate the network and security posture of *Critical BGP Prefixes* and *ASes* in five European countries: the Netherlands, Switzerland, Sweden, Lithuania, and Estonia.
3) We uncover jurisdictional hosting dependencies on foreign networks and persistent exposure to routing vulnerabilities that challenge European digital sovereignty.
4) We publicly release our methodology and datasets, promoting transparency and reproducibility [6].

Our findings offer actionable, data-driven guidance for enhancing the routing security and sovereignty of European Critical Infrastructure, bridging the gap between empirical Internet measurements and policymaking in the EU.

II. Related Work

CI vulnerabilities span across multiple layers, including physical infrastructure [7], [8], [9], [10], the underlying protocols (i.e., IP/TCP) [11], [12], [13], [14], and BGP itself [5], [15], [16], [17], [18]. Recent research has examined how vulnerabilities in interconnected systems can trigger cascading failures in *CI*. For instance, [19] investigated the causes and propagation of failures in power grids triggered by cyberattacks, while [12] highlighted how BGP-based traffic

ISBN 978-3-903176-82-9

manipulation and packet filtering were employed to implement large-scale Internet shutdowns in Egypt and Libya.

Quantitative methodologies have been developed to assess *CI* risks and cascading effects. Rehak et al. [20] introduced the SYNEFIA methodology to evaluate synergistic impacts of *CI* failures, demonstrating its application in the Czech Republic. Khadka et al. [21] developed a method to assess the security of AS paths towards Microsoft's email services, focusing on Route Origin Validation (ROV) protection. In [22], the authors assessed how much Dutch critical infrastructure depends on foreign Internet providers, using DNS and BGP data to map organizational dependencies. Kumar et al. [23] revealed trends in cross-border dependencies and centralization in government hosting infrastructures, while, Sommese et al. [24] analyzed the DNS resilience of e-government domains in four countries, finding widespread reliance on single DNS providers and limited use of IP anycast, especially in Europe.

While much attention has been devoted to securing industrial control systems (ICS) and physical infrastructure [25], [26], [27], [28], the role of BGP in sustaining *CI* has been less systematically studied. Existing work highlights broad systemic vulnerabilities [27], [28] but stops short of identifying which specific prefixes and autonomous systems (ASes) are most critical to essential services. Our work addresses this gap by mapping critical services to their supporting BGP prefixes, characterizing their network and security posture and providing insights to strengthen the resilience of *CI*.

III. Methodology

In this section, we detail our methodology to infer *Critical BGP Prefixes* and *Critical ASes* , as well as validate the input dataset to ensure the reliability of the inferred results.

A. Definitions

We define two key entities that form the basis of our analysis, namely, ***Critical BGP Prefixes*** and ***Critical ASes***.

A) ***Critical BGP Prefix*** is any publicly routed IP prefix originated by an entity that operates in a sector defined as critical under the EU NIS2 Directive (2022/2555) [1]. The 18 NIS2-defined critical sectors are:

1) Energy
2) Transport
3) Banking
4) Financial Market Infrastructure
5) Health
6) Drinking Water
7) Wastewater
8) Digital Infrastructure
9) ICT Service Management
10) Public Administration
11) Space
12) Postal and Courier Services
13) Waste Management
14) Manufacture, Production and Distribution of Chemicals
15) Production, Processing and Distribution of Food
16) Manufacturing
17) Digital providers
18) Research

B) ***Critical Autonomous System (AS)*** is an AS which originates at least one *Critical BGP Prefix* and is therefore responsible for the reachability of the critical services hosted within that prefix. Such ASes constitute the routing backbone of *CI* entities, for example those operated by governmental, healthcare, or financial institutions.

B. Overview

Our methodology for identifying *Critical BGP Prefixes* and *Critical ASes*, as outlined in Figure 1, is as follows:

1) ***Step 1: Domain-names Collection****:* The identification of *Critical BGP Prefixes* begins at the domain-level. Our approach leverages domain-names datasets from Basisbeveiliging.nl [29] and Hardenize.com [30], which provide lists of domains spanning both *CI* and *non-CI* sectors. In this work, we specifically focus on the Netherlands, Sweden, Switzerland, Estonia, and Lithuania as their coverage aligns closely with our study's scope (Europe). This selection is also driven by the availability of public, structured domain-level datasets with sufficient coverage for our measurement methodology and is therefore not intended to constitute a representative sample of the EU. The collected domains are: a) mapped to globally routable prefixes and b) filtered to capture only *CI* services (see Subsection III-C and Table I).

2) ***Step 2: DNS Resolution****:* DNS resolution is a fundamental step in mapping *CI* domains to the underlying network infrastructure that supports them. This involves querying authoritative DNS servers to resolve each domain into its corresponding IPv4 (A record) and IPv6 (AAAA record) addresses. To efficiently process large-scale queries, we use MassDNS [31], a high-speed resolver that enables rapid, parallelized lookups. For our DNS queries we leverage the full list of public resolvers provided by default with MassDNS to enhance query success rates and redundancy.

3) ***Step 3: Prefix and AS Matching****:* The next phase involves mapping the resolved IP addresses from Step 2 to their respective BGP prefixes and ASes using the Longest Prefix Match (LPM). Toward that goal, we leverage the CAIDA pfx2AS dataset [32]. This dataset is suitable for the task as it aggregates real-world routing table data, encompassing all publicly advertised IPv4/IPv6 prefixes and their owner ASes. We utilize Team Cymru's bogon lists [33] to filter out private, reserved, and unallocated prefixes, ensuring that only valid public BGP prefixes are included in the analysis.

C. Filtering and Validation

1) Business Sectors Filtering: To ensure that our analysis focuses exclusively on *CI* entities, we classified all *Critical ASes* from Step 3 based on their economic and organizational roles, using ASdb [34], a widely popular dataset. This classification step: a) allows us to filter out ASes that do not operate within *CI* and b) provides a first look into the distribution of the participating ASes across different sectors.

Guided by the sectoral taxonomy introduced in the EU NIS2 Directive [1] and referenced in Subsection III-A, we manually mapped each ASdb category to its corresponding NIS2 sector. The inferred ASes and their corresponding BGP prefixes that did not map to any NIS2-defined sector (e.g., Museums, Nonprofits, or Unknown) were designated as *Out of Scope* and were excluded from subsequent analyses to maintain alignment with the NIS2 framework.

Table I presents the resulting distribution of business types among *Critical ASes*. The majority fall under Computer and Information Technology, mapped to the Digital Infrastructure

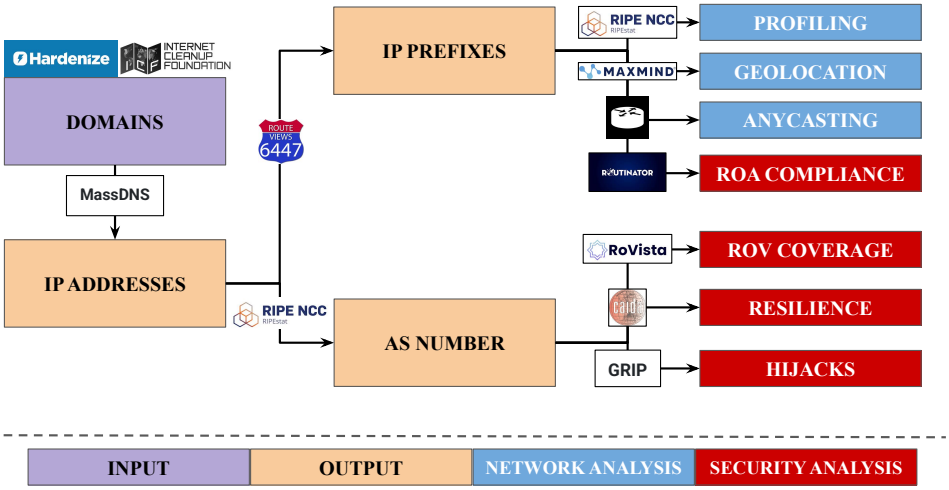

Fig. 1: The workflow begins with the identification of CI domains, which we then resolve into IP addresses using DNS resolution. We map these IPs to BGP prefixes through routing data, forming the foundation for further analysis. The color coding in the figure represents key phases of the methodology: the initial input and domain identification process (highlighted in purple), DNS resolution and data mapping steps (depicted in orange), and the final network and security analysis (shown in blue and red respectively).

Category	**Mapped NIS2 Sector**	**Count**
Computer and Information Technology	*Digital Infrastructure* and *Digital Providers*	933
Finance and Insurance	*Banking* and *Financial Market Infrastructure*	72
Utilities and Services (Excluding Internet Service)	*Energy*, *Health*, *Drinking Water*, *Wastewater* and *Waste Management*	53
Government and Public Administration	*Public Administration*	46
Media, Publishing, and Broadcasting	*Digital Infrastructure* and *Digital Providers*	34
E-commerce Sites	*Digital Infrastructure*, *Digital Providers* and *Financial Market Infrastructure*	23
Education and Research	*Public Administration* and *Research*	21
Manufacturing	*Manufacturing*, *Energy* and *Production, Processing and Distribution of Food*	15
Construction and Real Estate	*Manufacturing*	13
Freight, Shipment, and Postal Services	*Transport* and *Postal and Courier Services*	10
Health Care Services	*Health*	10
Agriculture, Mining, and Refineries	*Energy* and *Production, Processing and Distribution of Food*	3
Travel and Accommodation	*Transport*	2
Unknown	*Out of Scope*	23
Community Groups and Nonprofits	*Out of Scope*	22
Museums, Libraries, and Entertainment	*Out of Scope*	5

TABLE I: Distribution of business categories among *Critical ASes* and their mapping to NIS2 sectors. The table highlights the sectoral composition of European *CI*, showing that most *Critical ASes* belong to Digital Infrastructure entities such as ISPs, hosting providers, and cloud operators.

Country	**Total Domains**	**Unresolved Domains**	**Resolved IPs**	**Critical Prefixes**	**Critical ASes**	**Dom./IP**	**Dom./Prefix**	**Dom./AS**
Netherlands	76631	868 (1.1%)	48556	4056	843	1.58	18.89	90.90
Switzerland	876	1 (0.1%)	1468	724	248	0.60	1.21	3.53
Sweden	1084	2 (0.1%)	1165	628	224	0.93	1.72	4.84
Lithuania	953	0 (0%)	1569	321	101	0.61	2.97	9.44
Estonia	2888	3 (1%)	1167	278	99	2.47	10.39	29.17

TABLE II: Overview of *CI* domain datasets across the five studied countries after validation and mapping. The table reports the number of domains, unresolved domains, unique IPs, prefixes, and ASes, together with domain-to-resource ratios.

sector, emphasizing the central role of ISPs, hosting, and cloud providers in routing *CI* traffic. While these business types also appear frequently among *non-CI* ASes [34], their disproportionate representation here emphasizes the strong interdependence between BGP resilience and the cloud and ISP industries. Nonetheless, the long-tail of less-represented industries suggests that *Critical ASes* serve diverse critical sectors, including energy, healthcare, and transport.

2) Input Dataset Validation: To further ensure the integrity and completeness of our input domain datasets, we validate all entries by checking whether each domain resolves to at least one publicly routable IP address. Domains that fail to return any valid IP address are excluded, ensuring that our analysis is based solely on publicly reachable services.

Table II summarizes the composition of our validated datasets across the five studied countries, including the number of unresolved domains, unique IP addresses, prefixes, and ASes. It also reports the average ratios of domains per IP, prefix, and AS, offering a quantitative overview of dataset coverage and diversity across national infrastructures.

Our validation results (see *Unresolved Domains* in Table II) show that only a small fraction of domains fall into this category: 868 in the Netherlands, 1 in Switzerland, 2 in Sweden, none in Lithuania, and 3 in Estonia. Given this negligible proportion (0–1% per country), the validated dataset provides a reliable and comprehensive foundation for subsequent network- and security-level analysis.

IV. Measurement-based Results

In this section, we aim to understand how Europe's Internet-facing *CI* is structured and secured in practice. Specifically, we examine the network and security posture of the identified *Critical BGP Prefixes* and *Critical ASes* from Section III, focusing on their structural organization, jurisdictional exposure, and routing security status.

A. Network Posture Analysis

1) Characterization of Critical Prefixes and ASes: We begin by characterizing the distribution of *Critical BGP Prefixes* and *Critical ASes* to establish a baseline understanding of how Europe's *CI* is organized.

As shown in Table II, patterns in AS and IP allocation reveal differences in how critical resources are managed. Countries like the Netherlands and Estonia demonstrate high ratios of domains per AS, reflecting a centralized management model that may streamline operations and resource allocation. However, this concentration creates risks, as failures on key ASes could disrupt a large portion of *CI* services. Nations like Lithuania, Sweden and Switzerland, with lower domain per AS ratios, indicate a more distributed management approach that can promote redundancy but may result in underutilized resources. Estonia mirrors the Netherlands' centralized efficiency, further highlighting the trade-off between resilience and efficiency.

2) Anycast Practices: Building on the structural analysis above, we evaluate how *Critical BGP Prefixes* use anycast to improve redundancy and fault tolerance. Anycast enables the same service to be announced from multiple geographically distributed locations, improving latency and availability. To quantify anycast deployment, we rely on two independent datasets: BGP.Tools and LACES [35], [36].

Our measurements indicate that only a small fraction of *Critical BGP Prefixes* employ anycast: 4.23% according to BGP.Tools and 2.82% according to the LACES dataset. This limited adoption does not necessarily imply a weakness; rather, it reflects the service-dependent nature of anycast, which may be unnecessary or operationally complex for certain *CI* functions. Future work could explore which types of *CI* services most benefit from anycast and how deployment strategies influence resilience and performance.

3) Jurisdictional Dependencies: Geolocating *Critical BGP Prefixes* provides insights into the hosting and jurisdictional dependencies of *CI*, yet remains a non-trivial task due to the complexities of Internet routing [37], [2], [38]. This challenge is particularly relevant in Europe, where tensions have intensified concerns around digital sovereignty and dependence on foreign cloud or transit providers. Given these concerns, our objective was to estimate the jurisdictional footprint of prefixes associated with *CI* services, rather than to pinpoint the exact hosting locations.

Toward that goal, we queried the RIPEstat MaxMind GeoLite API [39], to obtain country-level geolocation data for each *Critical BGP Prefix* on November 1, 2024,. The MaxMind dataset derives geolocation information from a combination of registry records and active measurements, making it one of the most popular geolocation sources.

Fig. 2 presents the geographical distribution of *Critical BGP Prefixes* across all countries in our study. Each subfigure illustrates the concentration of geolocated prefixes in Europe and the United States, highlighting the jurisdictional dependencies of these networks. Our results align with prior observations on jurisdictional dependencies in *CI*. For example, [22] found that a significant portion of Dutch *Critical BGP Prefixes* are announced by foreign ASes, effectively making them dependent on external entities.

Our analysis reveals significant cross-border reliance on U.S.-based infrastructure. For each country under study, a significant fraction of *Critical BGP Prefixes* are geolocated within the United States (subfigures b–d). In detail:

US Concentration Estonia (b1) and Lithuania (b2) show a more distributed prefix presence, though the U.S. remains a dominant hosting location for their *CI* services. The Netherlands (b3) and Switzerland (d1) present a more balanced geographical distribution, but still reveal strong U.S. hosting footprints. Sweden (d2) stands out with a considerable proportion of prefixes hosted domestically, suggesting a more localized *CI* strategy.

EU Concentration Sweden (c2) shows a strong trend toward domestic hosting, evident in the high proportion of prefixes geolocated within its borders, which may contribute to a higher degree of network sovereignty. The Netherlands (a3) and Switzerland (c1) exhibit a more geographically distributed presence across Europe, likely reflecting their extensive regional peering ecosystems. Baltic countries such as Estonia (a1) and Lithuania (a2) display mixed geolocation patterns, with dependencies on both domestic and foreign European infrastructure.

Heavy reliance on U.S.-hosted prefixes could subject critical services to foreign regulations, legal orders, or data access policies, potentially impacting national security. These findings align with ongoing discussions on European digital sovereignty [40]. The European Commission and various

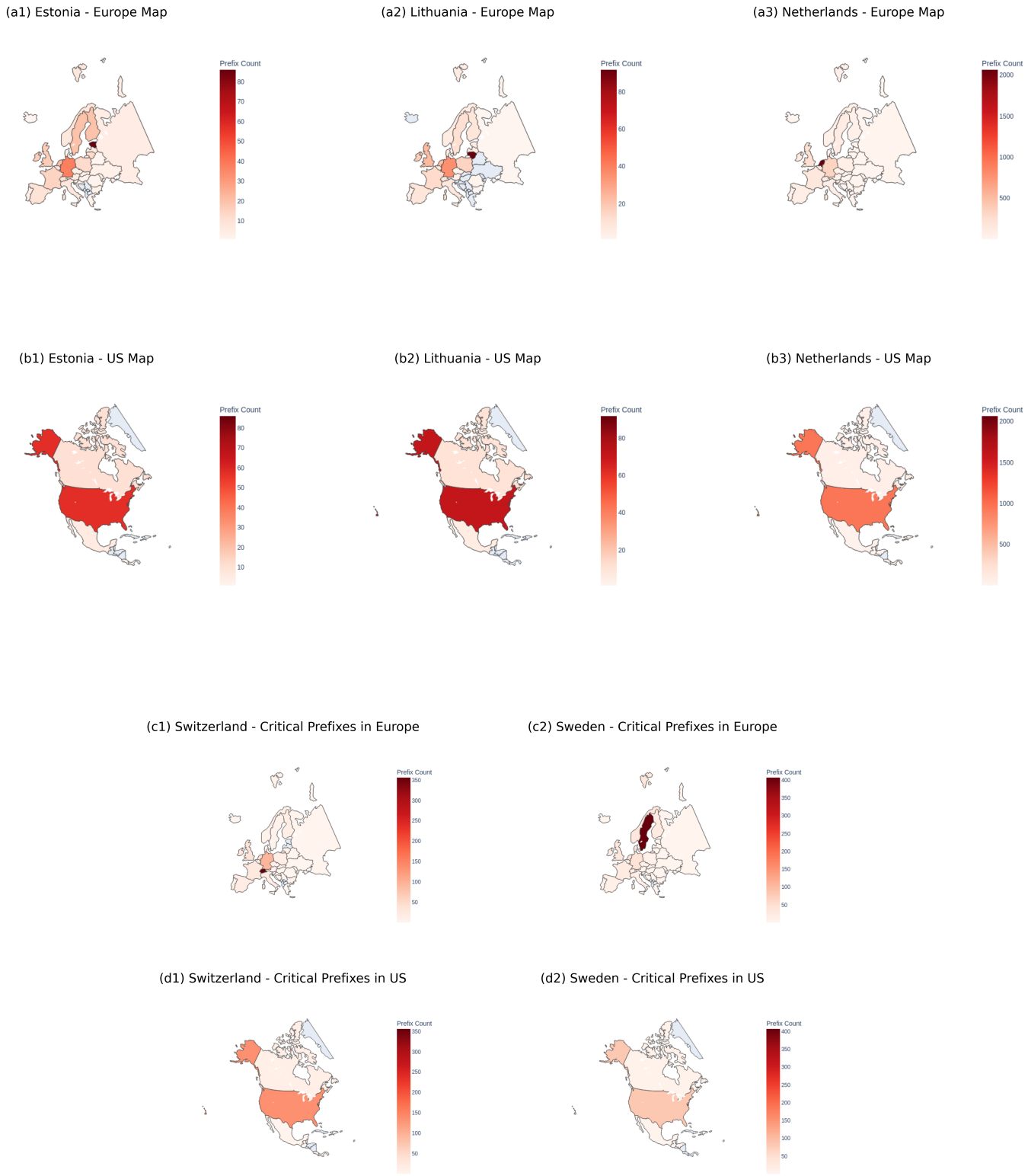

Fig. 2: Geographical Distribution of *Critical BGP Prefixes. Categories (a) and (c) correspond to presence in European-based headquarters, while, categories (b) and (d) correspond to US-based headquarters.*

national policymakers have emphasized the need to *reduce reliance on non-European infrastructure* and strengthen *regional cloud and network autonomy*. Initiatives such as *GAIA-X* aim to establish a federated European cloud infrastructure that minimizes dependencies on U.S. and Chinese providers [41]. **However, our results suggest that many European countries continue to rely on external hosting, raising concerns about long-term resilience in the face of geopolitical uncertainties.**

B. Security Posture Analysis

We next assess the routing-security exposure of *Critical ASes* through observed BGP hijack events. We use hijacks as a routing-layer security indicator because they can directly affect the reachability, traffic integrity, and path control of Internet-facing *CI* services associated with *Critical BGP Prefixes*. This analysis is not intended to characterize the full cybersecurity posture of *CI*, but rather to quantify routing-specific exposure within the scope of our BGP-focused measurement study. To that end, we examine prefix hijacks observed throughout the duration of 2024 through the Global Routing Intelligence Platform [42] API. GRIP detects Multi-Origin AS anomalies based on high-confidence scores.

Fig. 3 illustrates the relationship between the number of hijack incidents (x-axis, log scale) and their total duration in hours (y-axis) for each affected *Critical ASN*. Each point represents a single ASN, with its size and color scaled by the total hijack duration. The plot reveals several clear outliers. **AS23470** (ReliableSite.net) stands out dramatically, experiencing 69 hijacks with a cumulative duration approaching 200 hours. Other high-impact ASNs include **AS174** (Cogent) and **AS7018** (ATT), each experiencing over 25 and 50 hijacks respectively with total durations exceeding 300 hours. Notably, **AS16509** (Amazon), underscores the risks that even hyperscale providers face. A large cluster of ASNs remains in the lower-left quadrant, indicating low exposure in terms of frequency and duration. While these networks appear more resilient, it is important to consider that infrequent but long-duration hijacks may still pose severe operational risks, especially in *CI* contexts. These phenomena illustrate the need for preventive mechanisms to secure the routing fabric of European *CI*.

V. Discussion

Our measurements reveal substantial jurisdictional dependencies on foreign, particularly U.S.-based, infrastructure for Internet-facing *CI* services. While our methodology does not allow us to infer the specific organizational or procurement decisions behind each hosting choice, several factors may explain this pattern. Large cloud, CDN, DNS, and hosting providers offer mature operational capabilities, including high availability, DDoS protection, global reachability, managed security services, scalability, and compliance support. For *CI* entities, these capabilities may outweigh concerns about jurisdictional locality, leading to trade-offs between resilience, performance, cost efficiency, and digital sovereignty.

Reducing such dependencies does not necessarily require avoiding global providers entirely. European alternatives exist through domestic ISPs, European cloud and hosting providers, national research and education networks, public-sector shared services, and multi-provider architectures that combine local hosting with external redundancy [43]. Sweden's stronger domestic footprint suggests that lower foreign dependency is achievable, although our measurements cannot determine whether this results from policy choices, procurement practices, market structure, or stronger domestic provider capacity. Other countries could follow this direction by incorporating jurisdictional exposure into *CI* procurement requirements, encouraging multi-homing across European providers, and periodically auditing the routing and hosting dependencies of Internet-facing CI services.

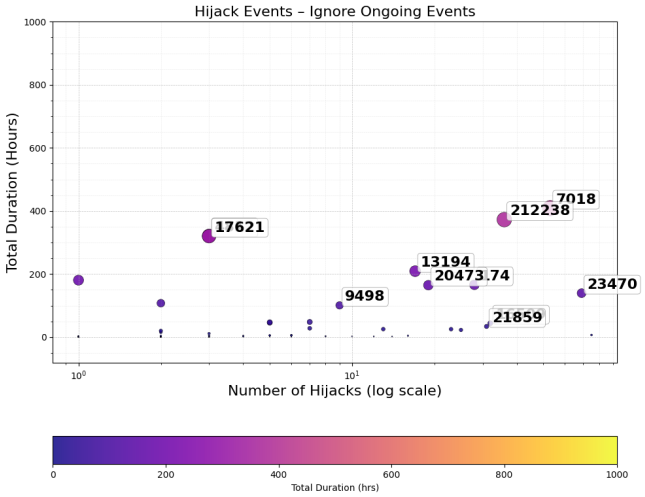

Fig. 3: Number of hijacks (log scale) VS. total hijack duration (in hours) for *Critical ASes* during 2024.

VI. Ethical Considerations

Our study exclusively relies on publicly available datasets. We do not perform intensive probing, interfere with operational infrastructure, or access confidential information.

VII. Conclusion

This paper presents a measurement-based analysis of the Internet-facing layer of European *Critical Infrastructure*. Across five European countries, our results show that this layer is often concentrated in a relatively small set of networks and providers, creating structural dependencies that may amplify operational risk. In addition, our analysis highlights substantial reliance on U.S.-based infrastructure and continued exposure to routing-security threats such as BGP hijacks, underscoring challenges for both resilience and European digital sovereignty.

As our study focuses on publicly visible services, it should be seen as a first step toward a broader understanding of *CI* Internet dependencies. Future work should incorporate internal dependencies, longitudinal routing dynamics and deeper analyses of mitigation mechanisms, enabling a more comprehensive view of how Europe can secure and strengthen the digital backbone that underpins critical services.

Acknowledgements

This research received funding from the Dutch Research Council (NWO) under the projects UPIN and CATRIN.

REFERENCES

[1] E. Commission, "Nis 2 directive: Eu cybersecurity measures directive (2022/2555)," 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

[2] S. Kastanakis, "The good, the bad, and the ugly of bgp routing modeling: Confounding factors, selective announcements and location-aware simulations," Ph.D. dissertation, Lancaster University, 2025.

[3] S. Kastanakis and C. E. Hesselman, "From policy to practice: A research agenda for measurement-based bgp risk assessment," in *10th Annual Cyber Security Next Generation Workshop, CSNG 2024*, 2024.

[4] Y. Rekhter, S. Hares, and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006.

[5] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in bgp security: A survey of attacks and defenses," *Computer Communications*, vol. 124, pp. 45–60, 2018.

[6] "Critical bgp prefixes dataset and code repository," https://github.com/kastanakis/critical-bgp-prefixes, 2026, accessed: 2026-04-30.

[7] Wikipedia contributors, "2008 Submarine Cable Disruption," 2024, [Online; accessed October 2025]. [Online]. Available: https://en.wikipedia.org/wiki/2008_submarine_cable_disruption

[8] NUPI - Norwegian Institute of International Affairs, "The Subsea Cable Cut at Svalbard, January 2022: What Happened, What Were the Consequences, and How Were They Managed?" "https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed", 2022, [Online; accessed October 2025].

[9] Wikipedia contributors, "2024 Baltic Sea Submarine Cable Disruptions," 2024, [Online; accessed October 2025]. [Online]. Available: https://en.wikipedia.org/wiki/2024_Baltic_Sea_submarine_cable_disruptions

[10] European Commission, "New Measures to Secure Submarine Cables and Critical Infrastructure," 2025, [Online; accessed October 2025]. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_580

[11] CNET News, "How Pakistan Knocked YouTube Offline—And How to Make Sure It Never Happens Again," https://www.cnet.com/culture/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/, 2008, [Online; accessed October 2025].

[12] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of country-wide internet outages caused by censorship," in *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, ser. IMC '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 1–18. [Online]. Available: https://doi.org/10.1145/2068816.2068818

[13] Imperva, "Session Hijacking: Attacks and Prevention Methods," Imperva Security Blog, 2025, [Online; accessed October 2025]. [Online]. Available: https://www.imperva.com/learn/application-security/session-hijacking/

[14] ThousandEyes, "China's New Weapon: The Great Cannon," ThousandEyes Blog, 2015, [Online; accessed October 2025]. [Online]. Available: https://www.thousandeyes.com/blog/chinas-new-weapon-great-cannon

[15] A. Siddiqui, "What happened? the amazon route 53 bgp hijack to take over ethereum cryptocurrency wallets," https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/, accessed: 2025-10-09.

[16] The Register, "Mystery Deepens Over Redirection of Internet Traffic Through Belarus and Iceland," The Register News, 2013, [Online; accessed October 2025]. [Online]. Available: https://www.theregister.com/2013/11/22/net_traffic_redirection_attacks/

[17] S. Servillo, P. Spadaccino, F. Cuomo, and F. Luciani, "Autonomous systems risk level in the route server infrastructure of an internet exchange point," in *2024 IFIP Networking Conference (IFIP Networking)*. IEEE, 2024, pp. 95–103.

[18] Mutually Agreed Norms for Routing Security (MANRS), "RPKI-ROV Deployment Reaches Major Milestone," MANRS Blog, 2024, [Online; accessed October 2025]. [Online]. Available: https://manrs.org/2024/05/rpki-rov-deployment-reaches-major-milestone/

[19] V. Subramaniam, A. Stefanov, A. Presekal, P. Palensky, and J. L. Rueda, "Cyber attacks on power grids: Causes and propagation of cascading failures," *IEEE Access*, vol. 11, pp. 103 154–103 176, 2023.

[20] D. Rehak, J. Markuci, M. Hromada, and K. Barcova, "Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system," *International Journal of Critical Infrastructure Protection*, vol. 14, pp. 3–17, 2016.

[21] S. K. Khadka, S. Bayhan, R. Holz, and C. Hesselman, "Assessing the security of internet paths: A case study of dutch critical infrastructures," in *Proceedings of the 2024 Applied Networking Research Workshop*, 2024, pp. 67–73.

[22] NLnet Labs, "How 'National' is the Dutch Critical IP Infrastructure?" 2013.

[23] R. Kumar, E. Carisimo, L. De Angelis Riva, M. Buzzone, F. E. Bustamante, I. A. Qazi, and M. G. Beiró, "Of choices and control – a comparative analysis of government hosting," in *ACM Internet Measurement Conference (IMC)*, 2024, pp. 1–18.

[24] R. Sommese, M. Jonker, J. van der Ham, and G. C. M. Moura, "Assessing e-government dns resilience," in *2022 18th International Conference on Network and Service Management (CNSM)*, 2022, pp. 118–126.

[25] J. Ceron, J. Chromik, J. Santanna, and A. Pras, "Online discoverability and vulnerabilities of ics/scada devices in the netherlands," 2019. [Online]. Available: http://hdl.handle.net/20.500.12832/2369

[26] S. J. Saidi, A. M. Mandalari, R. Kolcun, H. Haddadi, D. J. Dubois, D. Choffnes, G. Smaragdakis, and A. Feldmann, "A haystack full of needles: Scalable detection of iot devices in the wild," in *Proceedings of the ACM Internet Measurement Conference*, ser. IMC '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 87–100. [Online]. Available: https://doi.org/10.1145/3419394.3423650

[27] M. Nawrocki, T. C. Schmidt, and M. Wählisch, "Uncovering vulnerable industrial control systems from the internet core," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2020, pp. 1–9.

[28] G. Barbieri, M. Conti, N. O. Tippenhauer, and F. Turrin, "Assessing the use of insecure ics protocols via ixp network traffic analysis," in *2021 international conference on computer communications and networks (icccn)*. IEEE, 2021, pp. 1–9.

[29] Basisbeveiliging.nl, "Basisbeveiliging.nl datasets," https://basisbeveiliging.nl/datasets, accessed: 2026-01-30.

[30] Hardenize, "Hardenize dashboards," https://www.hardenize.com/dashboards/, accessed: 2026-01-30.

[31] Blechschmidt, Benni, "MassDNS: A High-Performance DNS Resolver," GitHub Repository, 2018, [Online; accessed October 2025]. [Online]. Available: https://github.com/blechschmidt/massdns

[32] S. D. CAIDA, University of California, "Routeviews prefix to as mappings dataset (pfx2as)," https://catalog.caida.org/dataset/routeviews_prefix2as, accessed: 2026-01-30.

[33] T. Cymru, "Team cymru bogon reference," https://www.team-cymru.com/bogon-reference-http, accessed: 2026-01-30.

[34] M. Ziv, L. Izhikevich, K. Ruth, K. Izhikevich, and Z. Durumeric, "Asdb: a system for classifying owners of autonomous systems," in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 703–719. [Online]. Available: https://doi.org/10.1145/3487552.3487853

[35] BGP.Tools, "Bgp.tools anycast prefixes dataset," 2026, accessed: 2026-01-30. [Online]. Available: https://github.com/bgptools/anycast-prefixes

[36] R. Hendriks, M. Luckie, M. Jonker, R. Sommese, and R. van Rijswijk-Deij, "Laces: An open, fast, responsible, and efficient longitudinal anycast census system," 2025. [Online]. Available: https://arxiv.org/abs/2503.20554

[37] S. Kastanakis, V. Giotsas, and N. Suri, "Understanding the confounding factors of inter-domain routing modeling," in *Proceedings of the 22nd ACM Internet Measurement Conference*, ser. IMC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 758–759. [Online]. Available: https://doi.org/10.1145/3517745.3563025

[38] S. Kastanakis, V. Giotsas, I. Livadariu, and N. Suri, "Replication: 20 years of inferring interdomain routing policies," in *Proceedings of the 2023 ACM on Internet Measurement Conference*, ser. IMC '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 16–29. [Online]. Available: https://doi.org/10.1145/3618257.3624799

[39] RIPE NCC, "RIPEstat API," 2026, accessed: 2026-01-30. [Online]. Available: https://stat.ripe.net/docs/02.data-api/maxmind-geo-lite.html

[40] European Parliament, "Digital Sovereignty for Europe," 2020, accessed: 2025-01-30. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651992

[41] G.-X. Association, "Gaia-x: A federated data infrastructure for europe," 2021. [Online]. Available: https://www.gaia-x.eu

[42] "Grip: Global routing intelligence platform," https://grip.inetintel.cc.gatech.edu/, 2026, accessed: 2026-01-30.

[43] EuroStack Directory Project, "Replace Big Tech with European Solutions," https://euro-stack.com/alternatives/, 2026, accessed: 2026-04-30.