90th Minute: A First Look to Collateral Damages and Efficacy of the Italian Piracy Shield

Raffaele Sommese*, Anna Sperotto*, Antonio Prado†, Jeroen van der Ham*, Antonia Affinito*
*University of Twente, The Netherlands; †Independent Consultant, Italy
{r.sommese, a.sperotto, j.vanderham, a.affinito}@utwente.nl, antonio@prado.it

***Abstract*—In the fight against illegal football streaming, Italy introduced Piracy Shield, a platform through which copyright holders can notify the national regulator (AGCOM), which in turn orders ISPs to block infringing resources – such as IP addresses and Fully Qualified Domain Names (FQDNs) – within 30 minutes. In this paper, we present the first investigation into the platform's real-world impact by reconstructing and analyzing its blocking activity. Our analysis shows that the platform causes significant collateral damage. Indiscriminate IP-level blocking has disrupted and continues to disrupt hundreds of legitimate, non-streaming websites. At the same time, the platform's effectiveness may have been undermined by streamers who evaded enforcement by migrating to new infrastructure and unfiltered IP address space. Based on these findings, we call on policymakers to critically reconsider the core principles in this blocking approach. The evidence suggests that its broad impact on legitimate services and the potential national security risks outweigh the intended benefits.**

I. Introduction

Illegal live streaming of football matches is considered one of the most damaging forms of digital piracy. Spain's LaLiga has estimated annual losses of around €200 million, along with the loss of thousands of jobs in the Spanish content industry due to streaming [1]. These figures have prompted leagues and regulators to adopt increasingly aggressive countermeasures. Several countries have introduced dynamic blocking systems to disrupt these streams in real time. La Liga obtained a court order requiring ISPs to block pirated streams, while France has been blocking illegal sports streams since 2022 and recently passed legislation enabling immediate, real-time intervention [2], [3]. Such time-sensitive measures often raise policy concerns, especially around the risk of overblocking. The Spanish system, for example, inadvertently affected numerous legitimate websites hosted on CloudFlare. Questions also remain about the actual effectiveness of blocking, with many likening it to a *whack-a-mole* game that streamers continuously evade, leaving the root problem unaddressed.

In this context, Italy launched the *Piracy Shield* platform, a system adopted by the national communications regulator, AGCOM [4]. Mandated by Italian Law 93/2023 [5], the platform requires ISPs to block reported IP addresses or Fully Qualified Domain Names (FQDNs) within 30 minutes, following a notification by authorized rightsholders, without any ex-ante assessment by the ISP. Despite unanimous political support, its operation has been highly controversial, especially following high-profile incidents in which thousands of legitimate websites hosted on a CDN – and even core Google services – were blocked. Until now, no empirical data has been available to evaluate the actual impact of Piracy Shield. Although AGCOM enforces blocking orders via Piracy Shield, the list of affected IP addresses and domain names is not publicly disclosed. This absence of publication is not formally justified in the available documents, but may stem from operational considerations (*e.g.,* to avoid circumvention by infringers), lack of a legal mandate to publish, and a regulatory balance that favors enforcement efficiency over full transparency. This paper presents the first data-driven investigation into the platform's efficacy and unintended consequences. By reconstructing and analyzing the set of blocked resources from a leaked GitHub public source, we shed light on Piracy Shield's operation and the extent of the collateral damage it causes to legitimate Internet services. We also question its effectiveness in curbing illegal streams, as evidence suggests that operators may evade blocking.

Our data paints a concerning picture, with hundreds of legitimate websites affected, leased address space rendered unusable, and risks emerging even for national infrastructure. In light of these findings, we urge authorities to reconsider the platform's core principles and to explore more viable, transparent approaches to combating illegal streaming.

II. Background and Related Work

A. IP and DNS blocking

Blocklisting is a technique that prevents access to online resources [6]. The reasons for implementing blocklisting can be of different nature, ranging from protection against malicious actors or undesired traffic (*e.g.,* a website blocking traffic from specific crawlers [7]), to protecting young Internet users from unsuitable content (e.g. parental control [8]), to securing a network [9], to preventing user to access specific resources (*e.g.,* censorship [10]–[13]). From a technical point of view, two well known ways to implement blocklist are IP and DNS blocking. In the first case, traffic is dropped if the source/destination IP address (depending on the use) matches a list of known offending IPs. In the second case, DNS requests regarding a sensitive resource are manipulated in a way such that they are either dropped, or the returned IP address is not the one of the original resource, effectively blocking access [14]. Blocking has sparked discussion also at the policy level, as it has been recognized that circumvention is at times easy, while there is often collateral damage [15], [16].

978-3-903176-75-1 ©2025 IFIP

B. Anti-Piracy initiatives

According to Interpol, "digital piracy refers to the illegal copying or distribution of copyrighted material via the Internet" [17], and examples are given in the fields of industries like film, TV, publishing and gaming. In this context, a specific type of copyrighted material that has sparked multiple and particularly aggressive anti-piracy initiative is sport events streaming, football in particular. Alongside Italy, the Spanish La Liga (major soccer league), together with Telefonica, who has acquired the streaming right for the games, have obtained a court order forcing Internet providers to block live pirated streams [2]. Similarly, France was already regularly blocking pirated streams since 2022, implementing a blocking system that combines observed infringement by a copyright-holder, verification by the French Regulatory Authority for Audiovisual and Digital Communication (ARCOM), and blocking by ISPs [18]. Blocking is always done for a specific amount of time, which is probably the reason that there are limited complains of collateral damage for the French case. Unfortunately, France has now passed a bill that enables immediate blocking [3]. Collateral damage, or overblocking, seems to be the common denominator among anti-piracy initiative that have a strong timing constraint. The Spanish initiative caused, for example, the block of several legitimate website on shared Cloudflare infrastructure [2]. Wrangling with similar issue about massive illegal streaming, the UK took instead a refreshing angle by targeting awareness and education, with the BeStreamWise campaign[1]. It remains an open discussion if anti-piracy blocking mechanisms are effective or not, as they are akin to a whack-a-mole game rather than addressing the root cause. An example is the study in [19], which investigated the Dutch court-mandated blockade against the piracy website The Pirate Bay (TPB). The study showed, by measurement, that there have been no impact in the percentage of Dutch population still accessing material on TPB, thus proving that the blockade was not effective.

C. History of Piracy Shield

Piracy Shield is a platform adopted by the Italian communications regulator AGCOM — following a public donation — to combat illegal streaming, especially of live sports events, in Italy [4]. It was established under Italian Law 93/2023, approved on 14 July 2023 with unanimous support from both chambers of Parliament, which laid the legal framework of the Piracy Shield system. The law specifically mandates that ISPs must block, within 30 minutes, any IP addresses or FQDNs involved in illegal streaming activities, as reported through the platform by copyright owners [5].

AGCOM was tasked by the Italian government to deploy and maintain the platform, which was originally donated by SP Tech, an Italian IT firm closely associated with Studio Previti, a legal consultancy specializing in intellectual property and media law. The platform was initially built to support up to 18,000 blocked FQDNs and 18,000 blocked IP addresses, and required copyright holders to submit *tickets* containing the resources to be blocked (IPs or FQDNs), along with forensic proof of the illegal streaming activity. For archival purposes, this evidence is stored, but blocking is carried out automatically, without any ex-ante assessment by AGCOM or ISPs. The requesting rightsholder bears full responsibility for the accuracy and legal validity of the claim, in accordance with Article 2(4) of Law 93/2023.

Italian ISPs were instructed to develop their own system to query the platform and implement a blocking strategy within 30 minutes of a request. At launch, there was no mechanism to request unblocking of a resource. Less than a month into operation, on 1 February 2024, the platform caused its first major collateral damage: an IP address belonging to the CDN Cloudflare was blocked, rendering more than 40,000 websites unreachable from Italy [20].

The law was modified in October 2024 [21], introducing the notion that IPs and FQDNs can be blocked if they are used *predominantly*–not necessarily exclusively–for illegal activities. Unfortunately, the law does not define what *predominantly* means in practice. The revision also extended the filtering requirement to VPN and DNS providers, regardless of their geographic location. To the best of our knowledge, only Google Public DNS [22] has begun complying with this rule.

The update also introduced an unblocking procedure: owners of blocked resources can request AGCOM to lift the block within a maximum of five days, provided they demonstrate no illegal activity is taking place. However, the list of blocked resources is not publicly available. Multiple Freedom of Information Act (FOIA)-equivalent requests filed by Italian users to access the list have reportedly been rejected by AGCOM. The lack of a public list makes it extremely difficult for resource owners to know that they have been subject to blocking.

Later, on 19 October 2024 at 18:56, a copyright holder submitted a blocking request for a subdomain of the CDN of Google – `drive.usercontent.google.com` – that supports the functioning of Google Drive and Youtube. As consequence, the two services were blocked in Italy for several hours. The block was lifted several hours later but due to DNS caching, the effects of the block persisted throughout the next day [23]. This incident was widely reported in national [24], [25] and international [26] media and was also cited as an example of overblocking in an ICANN SSAC report [16].

In March 2025, AGCOM extended the scope of Piracy Shield beyond football to include live movies and TV series [27]. Several critics warned that Piracy Shield may breach the EU's Open Internet Regulation and the DSA by imposing blanket blocks on shared IPs, risking collateral damage to lawful services without judicial oversight, a concern also raised by the EU Commission in its comment to the Italian government [28]. Dissent also emerged within AGCOM itself. Commissioner Elisa Giomi publicly called for the suspension of the platform after major overblocking incidents [29]–[31]. Furthermore, several actors claim that Piracy Shield has been ineffective in converting pirates into paying subscribers, casting doubt on its overall impact as an anti-piracy measure [32].

[1] https://bestreamwise.com

III. Datasets and Methodology

A. Identifying blocked resources

To assess the effectiveness and potential collateral damage of the blocking measures enforced by the platform, our first step was to identify the list of blocked resources. Unfortunately, as discussed in section II, AGCOM does not publish a comprehensive list of IP addresses and FQDNs subject to blocking. Only in 2025 AGCOM introduced a website [33] that allows verification of the blocking status of individual resources (either IP addresses or FQDNs).

Another oracle-like source operating under a similar principle is managed by an Italian ISP: Infotech. This operator also offers a website interface for verifying the blocking status of specific IPs or FQDNs. Additionally, Infotech publicly releases a list of "tickets" – the content holder blocking requests – indicating the number of IPs blocked per ticket, along with anonymized data—IPv4 addresses are redacted in the last two octets, and FQDNs are truncated by six characters [34].

However, neither of these sources provides a complete list suitable for large-scale analysis. To overcome this limitation, we explored a dataset leaked on GitHub [35], which has been referenced several times in Italian network operator channels. The dataset contained, as of June 4, 2025, 10,918 IPv4 addresses and 42,664 FQDNs. Although the repository claims: "*This won't help much as the data is randomly generated and not real data*", the update frequency and the volume of blocked resources closely match statistics published by Infotech.

To validate the authenticity of the leaked list, we cross-referenced it against both the AGCOM and Infotech websites. Due to the presence of a CAPTCHA on the AGCOM website, we manually verified only the first 7,624 IP addresses (covering blocks issued up to February 4, 2025). In a few instances where AGCOM reported an IP as unblocked, we observed via Infotech that the block had indeed been previously applied and later removed. As the blocking status and dates otherwise aligned, we considered Infotech sufficiently trustworthy and relied on its website for further validation.

This process led to the construction of a validated list comprising 10,918 IPv4 addresses. Among these, 10,766 (98.6%) were confirmed still to be blocked, while for only 152 (1.4%) the block was revoked. As June 4, 2025 the website of Infotech reports 10,835 active IPv4 blocks, bringing us to 99.5% coverage of the blocked IPs. For IPv6, despite the support, no address has been reported to be blocked by the platform. Regarding FQDNs, we verified 42,654 domains from the leaked list. Of these, 18,849 (44.2%) were confirmed as still blocked, and 23,805 (55.8%) had been removed. Also in this case, as June 4, 2025 the website of Infotech reports 20,005 active FQDNs blocks, bringing us to 94.2% coverage of the blocked FQDNs.

While this dataset may not be exhaustive – particularly with respect to resources blocked prior to the start of Infotech's statistics collection – it nonetheless provides a conservative lower-bound estimate of the platform's blocking activity, which serves as the foundation for the subsequent analyses.

Having identified a validated list of blocked IPs and domains, we next explore the characteristics of these resources.

B. Inferring Leasing Activity

As second step, we aimed to understand the ownership and operational control behind blocked resources. During our initial investigation, we observed that a significant number of IP addresses appeared to belong to leased address space. We decided to delve into this aspect due to the fact that leasing can facilitate evasion tactics employed by illegal streamers, and create possible collateral damages after the end of the lease to other leases. To verify this hypothesis, we correlated the collected IP addresses with a curated longitudinal dataset of inferred leased prefixes, made available on request by the authors of [36], [37]. The dataset includes inferred leasing information with quarterly granularity from January 2024 to September 2024, and monthly granularity until May 2025. The leasing inference of [36], [37] provides a lower-bound estimation, as missing Internet Routing Registry information may cause the methodology to classify some leased addresses as non-leased. For further details, we refer to the original papers. Due to the relatively coarse temporal resolution, we considered an IP address as leased during the blocking period if it was marked as leased in either the snapshot immediately preceding or following the date of the block.

C. Inferring Hosting Activity

To assess the potential collateral damages introduced by the platform, we leveraged data provided by OpenINTEL [38] to identify domains either hosted on blocked IP addresses or referring – via CNAME records – to blocked FQDNs. OpenINTEL is a large-scale DNS measurement platform that conducts daily scans of approximately 80% of the second-level domain (SLD) namespace.

For this analysis, we considered ≈262 million domain names from several popular top-1 million rankings (i.e., Tranco, Umbrella, Radar), all the ICANN Centralized Zone Data Service (CZDS) gTLDs (such as `.com`, `.net`, `.xyz`, etc.), and multiple ccTLDs—both openly accessible (e.g., `.se`, `.ch`) and those accessible under NDA (e.g., `.nl`, `.ru`). OpenINTEL also collects ccTLDs domains observed in Certificate Transparency Logs (CT Logs) [39]. However, due to a recent internal restructuring of the dataset, we were unable to use this source. Additionally, OpenINTEL does not typically resolve names beyond the SLD level (*e.g.,* `foo.bar.com`), except for selected common labels such as `www`.

To overcome these limitations, we conducted a one-time scan of ≈1.8 billion FQDNs extracted from CT Logs [40], targeting certificates issued between January 1, 2024, and June 1, 2025. We excluded certificates issued prior to 2024 in order to focus on recent and active infrastructure, thereby avoiding stale or inactive names. As discussed in [39] (Section 4.2), this may result in a partial loss of visibility; however, given our objective of establishing a conservative lower-bound estimate of collateral damage, we accepted this trade-off.

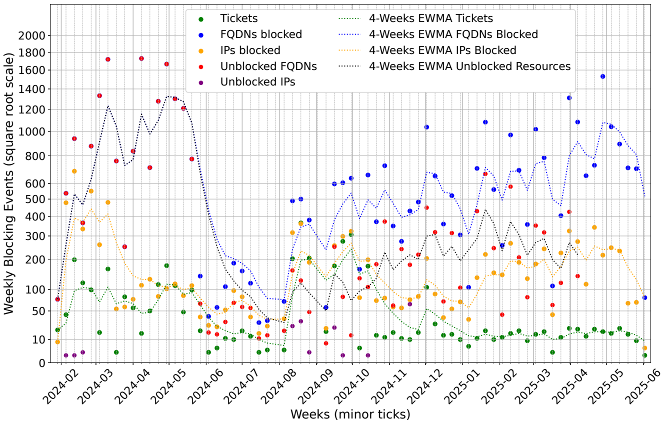

Fig. 1: Weekly blocking and unblocking events with 4-weeks Exponentially Weighted Moving Average (square-root scale)

Finally, we incorporated OpenINTEL's infrastructure measurements, which map domain names to their authoritative nameservers and mail server IP addresses. Since many unrelated domains may share DNS or mail infrastructure, blocking an IP hosting such services can cause unintended side effects. We used this data to evaluate potential collateral damage to DNS and mail hosting infrastructure.

IV. Results

A. *Blocked Infrastructure*

From February 2, 2024 to June 4, 2025, a total of 3,782 blocking requests – also referred to as *tickets* – were issued on the Piracy Shield platform. Of these, 1,817 (48%) targeted both at least one FQDN and one IPv4 address, 1,719 (45%) targeted only FQDNs, and 246 (7%) targeted only IPs.

Blocking tickets are predominantly issued during weekends, with 38% of requests occurring on Sundays, 30% on Saturdays, and 12% on Fridays. Monday is the weekday with the highest number of tickets (13%), followed by Tuesday (3%), Thursday and Wednesday (2%). The only notable exception to this pattern is Monday, August 19, 2024, which saw a sharp increase with 130 tickets issued on that single day.

Looking at the number of blocked resources (*i.e.,* IPs and FQDNs), we observe a similar weekly pattern. In terms of broader temporal trends, on the platform copyright-owner issued an average of 7.75 tickets per day, along with an average of 87.41 FQDNs and 22.37 IPs blocked daily. The number of tickets, IPs, and FQDNs grew more rapidly in the first four months of 2024. Activity dropped below average in June and July (Figure 1), which coincides with the pause period of the Italian National League, and returned to average levels in the following months through June 2025.

There are two main exceptions to these patterns. First, a spike in ticket volume occurred in August 2024, although these tickets blocked fewer resources per request. Second, IP blocking was more pronounced at the beginning of 2024 compared to the remainder of the period.

Finally, when looking at unlocked FQDNs, we find that most of them were originally blocked in early 2024. A likely explanation is a technical limitation initially imposed by the platform on the maximum number of blocked FQDNs, which led AGCOM to unlock older resources to stay within system constraints.

TABLE I: Statistics on blocked IPs, their relative /24 prefixes, and unblocked IPs per ASN

ASN	Name	#IPs (% total)	# /24s	#Unblocked IPs
142019	GZ Remittance	1,035 (9.5%)	15	1
62390	NexonHost	834 (7.6%)	31	6
16276	OVH	719 (6.6%)	494	41
214785	369 IntoNet	610 (5.6%)	6	1
25198	ZetServers	452 (4.1%)	35	9
64286	LogicWeb	408 (3.7%)	7	0
141718	IPv4 Superhub	406 (3.7%)	19	1
58349	INNETRA PC	295 (2.7%)	8	2
30860	Virtual Systems	261 (2.4%)	35	2
12876	SCALEWAY	260 (2.4%)	169	4
43139	Maximum-Net	258 (2.4%)	3	0
215224	NovoServe	226 (2.1%)	26	2
24940	Hetzner	191 (1.8%)	162	3
60064	Hostpalace	171 (1.6%)	11	4
47674	Net Solutions	161 (1.5%)	14	3
–	Others	4,631 (42.4%)	1,099	73
–	Total	10,918 (100.0%)	2,134	152

1) Blocked IPs: Shifting our focus to IPs, we investigated the distribution of blocked addresses across /24 networks, ASNs and Countries using IPInfo dataset [41]. The 10,918 blocked IP addresses span 2,134 /24 networks and 262 ASNs. In Table I, we report the top 15 hosting infrastructures for all IPs that were ever blocked, either currently or in the past. Interestingly, a single company – GZ Remittance—hosted more than 9.5% of all blocked resources, concentrated in just 15 distinct /24s. This may suggest that the company is highly favored by illegal streaming operators, who likely rotate through IPs to evade blocking. The same pattern is observable for NexonHost, which shows similar figures.

Well known hosting providers, such as OVH, Scaleway, and Hetzner, exhibit a different blocking pattern. Streamers here appear to rely on shared pools of IPs, resulting in blocks spread over a more diverse set of /24s. In particular, OVH stands out for having the highest number of unblocked IPs – 41 in total, accounting for almost one third of all unblocked addresses. This suggests that shared resources may have been inadvertently affected, or that the infrastructure was later reused for benign purposes.

Additionally, looking beyond the top 15 hosting infrastructures, we observe a long tail of providers with only a few blocked addresses per ASN. Among these, we highlight several noteworthy cases that remain blocked to this day: 94 IPs associated with Akamai, 3 with Incapsula – both large content delivery network – and 47, likely leased, with an Iranian educational /24 network. In subsection IV-C, we further examine whether blocking IPs may result in collateral damage.

The hosting country perspective (Table II) shows that 37.9% of the IPs blocked by Piracy Shield are hosted in the Nether-

TABLE II: Distribution of blocked IPs per country

Country	#IPs	Country	#IPs
NL	4,135 (37.9%)	SE	634 (5.8%)
DE	985 (9.0%)	GB	396 (3.6%)
RO	898 (8.2%)	IT	275 (2.5%)
US	843 (7.7%)	HK	265 (2.4%)
UA	676 (6.2%)	Others	1,175 (10.8%)
FR	636 (5.8%)	Total	10,918

lands, followed by Germany (9.0%) and Romania (8.2%). Interestingly, 2.5% of the blocked IPs are located in Italy, and 76.8% of the blocked IPs are within the European Union, where copyright owners may have better leverage to identify illegal streaming perpetrators and take them down.

Finally, we have also examined the number of blocked IPs that are still active by probing them with Nmap. Out of 10,914 blocked IPs, 5,588 (51%) were still responsive. This may potentially indicate that the remaining IPs have been abandoned, repurposed, or that illegal streaming operators have since migrated to different infrastructures.

TABLE III: Distribution of blocked FQDNs per TLDs

TLD	#FQDNs		TLD	#FQDNs	
	Blocked	Unblocked		Blocked	Unblocked
com	8427 (19.8%)	4302	cc	1211 (2.8%)	699
xyz	6805 (16.0%)	4080	info	1070 (2.5%)	232
me	6569 (15.4%)	3985	top	957 (2.2%)	271
net	3371 (7.9%)	2408	live	722 (1.7%)	460
org	2082 (4.9%)	1585	Others	9746 (22.8%)	4938
pro	1694 (4.0%)	845	Total	42654 (100.0%)	23805

2) Blocked FQDNs: For FQDNs, as mentioned earlier, 42,654 were blocked across 275 TLDs and 13,294 registered domains. Of these FQDNs, 18,849 remain blocked as June 4, 2025. The top 10 TLDs (Table III) account for 77.8% of all time blocked FQDNs, with `.com` leading at 19.8%, followed by `.xyz` at 16.0% and `.me` at 15.4%.

Looking at unblocked resources, some TLDs, *e.g.,* `.top`, appear to have fewer unblocks. However, as previously noted, early blocked FQDNs were more likely to be released in order to overcome platform limitations, and these differences may simply reflect variations in registration campaigns.

Turning to SLDs, one immediate standout is `ddns.net`, a free dynamic DNS operated by the No-IP service, which hosted 4.0% of the blocked FQDNs. Aside from this outlier, the distribution of FQDNs per SLDs follows a long tail.

We also investigated how many of the FQDNs are still active and resolvable with an IPv4 address. Out of the 18,849 FQDNs still blocked, 16,925 remain resolvable, while 1,924 are unresolvable. In general, we observed that unresolvable FQDNs tend to have an earlier blocking date – on average, three months prior – suggesting that illegal streamers may abandon older resources over time.

Among the unblocked FQDNs, we found that out of 23,805 entries, 15,552 are still resolvable, while 8,253 are not. Unfortunately, we have no way of determining whether illegal streaming activity has ceased on the resolvable but unblocked FQDNs, or whether PiracyShield was forced to remove them solely due to technical limitations. We also collected creation dates for the registered domains associated with 13,066 unblocked FQDNs and 11,873 still blocked FQDNs via the Registration Data Access Protocol (RDAP). Among these, we found that 154 of the unblocked domains and 119 of the still blocked ones were re-registered after their corresponding blocking dates, indicating potential overblocking caused by aging entries in the blocked list. We also observed that the median time difference between domain creation and FQDNs blocking is 603 days. However, this value is skewed by cases where illegal streamers, as shown in the case of No-IP, leverage free third level domain registration services. In such cases, the parent second level domain is legitimate, long-lived, and often used for benign purposes.

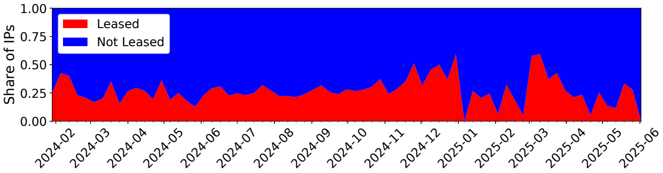

Fig. 2: Shared of leased IP addresses blocked weekly

B. IP Leasing Prevalence

After investigating the general trends of blocking on the platform, we shift our focus to understand if the blocked IPs belongs to leased IP address space.

Out of 10,918 blocked IPs, 2,618 (24%) were leased. This result, while still a lower-bound estimate due to the limitations of the approaches proposed by [36], [37], indicates that streamers heavily leverage indirectly IP leasing, via their hosting companies or directly by themselves, to obtain addresses for their services. We reached out to IPXO, a market-leader IP leasing broker, that confirmed an additional 330 blocked addresses (3%) belonging to leased /24s on their marketplace in addition to our insights. We included those addresses in our analysis. In Figure 2, we observe that the number of blocked leased IPs exceeds half of all blocked IPs in some weeks. We also found that, on average, 7.5 IPs per /24 are blocked in leased address blocks, compared to 4.5 in non-leased blocks. This suggests that illegal streamers may attempt to exploit leased address space more intensively, even if just indirectly, by obtaining them by hosting companies that leases them, leading to more potential collateral damages for new lessees.

Looking at the top 10 hosters in Table I, we observed that on AS58349 (INNETRA PC), 85% of the blocked IP addresses were leased, followed by AS215224 (Novoserve) with 67%, AS47674 (Net Solutions) with 49%, and AS62390 (NexonHost) with 46%. Other top providers show significantly lower percentages, indicating that leasing may be a practice adopted primarily by specific groups hosters.

We also found that a non-negligible 4% (453) of the addresses were leased after being blocked and were not originally leased. This may indicate resources previously abused by streamers and later made available on the leasing market to

TABLE IV: Distribution of active collateral damages by type and impact

Blocked Resource	FQDN collateraly blocked		Confirmed non-streaming	
	Completely	Partially	Completely	Partially
cname	240	59	2	0
cname ∩ ip	82	20	0	0
ip	6027	188	373	14
ip ∩ mx ip	187	4	32	0
ip ∩ mx ip ∩ mx ip	28	1	6	0
ip ∩ ns ip	3	32	1	0
mx ip	142	10	69	3
mx ip ∩ mx name	1	0	0	0
mx name	2	0	0	0
ns ip	0	87	0	10
ns name	0	1	0	0
Total	6712	402	483	27

users unaware of the collateral damage they face by having those IPs blocked in Italy. Of those addresses, only 2 have been removed from the blocked list, while 451 remain blocked.

With the help of IPXO, we further investigated whether, after the blocking date, leased prefixes changed ownership, potentially indicating collateral damage to new customers. We found that, out of 1,012 IPs spanning 121 /24s leased on their marketplace and still subject to blocking by the Piracy Shield platform, 268 IPs (across 32 /24s) are no longer leased by the same companies, and 250 IPs (across 23 /24s) have been re-leased to different companies. Furthermore, 3 IPs (from 3 distinct /24s) have been removed from the leasing marketplace and returned to their original owners.

These results highlight a significant risk of collateral damage for companies that may find part of their address space unusable when communicating with Italian customers.

C. Collateral Damages

In the previous section, we showed how IP addresses can change ownership due to IP leasing. The nature of the services hosted on these IPs may also vary over time, and multiple websites can be hosted on the same address at same time. To investigate the potential damages arising from this, we used DNS data as described in subsection III-C. First, we examined collateral damage that is still active today, using OpenINTEL data and our CT log–seeded FQDN scan. Second, we investigated longitudinal collateral damage over the entire analysis period, limited to domain names measured by OpenINTEL, for which historical data is available.

Within the OpenINTEL dataset, we checked whether the blocked IPv4 addresses appeared in the set of IPv4 addresses (i.e., `A` record responses) for specific domain names (`ip` in Table IV), or in the IPs associated with mail server or name server records (`mx` and `ns`). If all associated IPs were blocked, we marked the domain as completely affected; otherwise, we marked it as partially affected. For FQDNs, we adopted a similar approach by checking for `CNAME` referrals (i.e., domains pointing to a blocked FQDN), or pointers to blocked mailserver or nameserver hostnames (`MX` and `NS` records, respectively). In the case of the CT log–seeded FQDN scan, we examined either the IPv4 records of the specific FQDN or whether the FQDN pointed to another FQDN that was blocked.

TABLE V: Top 10 languages found in active, collateral-damaged, confirmed non-streaming FQDNs

Language	Count	Language	Count
English	237	Polish	11
French	99	Italian	9
Spanish	60	Portuguese	8
German	29	Arabic	7
Albanian	19	Others	26
Indonesian	5	Total	510

Finally, from the list of FQDNs identified as potential collateral damage, we excluded all FQDNs that were explicitly blocked by the Piracy Shield platform–either currently or in the past–under the assumption that any FQDN blocked by the platform was indeed associated with illegal streaming activity and therefore does not constitute collateral damage.

For the active collateral damages, we identified a total of 7,114 FQDNs spanning 5,228 SLDs and 176 TLDs that are either completely or partially affected by blocking activities. Among these, 1,931 responded to HTTP or HTTPS requests. We manually inspected the landing pages to classify these domains and distinguish those unrelated to streaming. As a result, we identified 510 non-streaming-related websites, 617 streaming-related websites, and 804 websites for which we were unable to determine the category (e.g., domain parked, access denied, and other similar cases).

We consider the 510 non-streaming-related websites as collateral damage caused by the platform and investigated them further. As shown in Table IV, only 2 instances of collateral blocking resulted from direct FQDN blocking by Piracy Shield, while the vast majority originated from IP-level blocking. Specifically, 131 blocked IP addresses are responsible for 508 collateral blockings. In three cases, a single IP address alone caused more than 60 collateral blockings.

The table also shows that in most cases (373 FQDNs), the IP block completely disrupted the operation of the affected domain, indicating full collateral impact.

Looking at the language distribution of websites associated with collaterally blocked FQDNs (Table V), we found that, beyond English, the vast majority are in French, Spanish, and German. This result is unsurprising, given the presence of OVH and Hetzner – two widely used European hosting providers – who may have unknowingly re-assigned or co-assigned abused IP addresses to new customers after those IPs were blocked by Piracy Shield. A quick analysis of the blocked IPs confirmed this hypothesis.

During our classification process, we observed a wide range of website types across these collaterally affected domains, including personal branding pages, company profiles, and websites for hotels and restaurants. One notable case involves 19 Albanian websites hosted on a single IP address assigned to WIIT Cloud. These sites are still unreachable from Italy.

The most relevant case for Italian users involves nine domestic websites that were collaterally blocked. Among them, we identified an Italian marketing company hosted on an OVH IP address currently blocked by Piracy Shield, making it completely unreachable from within Italy. Other affected websites include those of a car mechanic, a nunnery, several retail shops, an accountant, and a telehealth missionary program. They relied on two IP addresses for their authoritative nameservers, one of which has been blocked, leaving the domain vulnerable to outages or attacks on the remaining IP.

These results, while being a lower-bound estimation, highlight that blocking IP addresses and FQDNs, can have unintended and potentially severe consequences, leading to collateral damage well beyond the original scope of the blocking and may disrupt national and international businesses.

Looking at historical collateral blocking, we found that, excluding the FQDNs still affected today as reported in Table IV, a total of 7,742 FQDNs were impacted by collateral blocking[2] between February 2024 and June 2025. As in the case of active collateral blocking, the vast majority originated from IP-level blocking: in 7,232 cases, all hosting IPs of the affected FQDNs were blocked, while in 302 cases only a subset of the hosting IPs were blocked. In addition, 782 FQDNs had their mail server IPs blocked, and 397 FQDNs were affected due to blocked nameserver IPs.

Among the latter, 325 FQDNs pointed one of their nameservers to a Hetzner IP address that was blocked by Piracy Shield in early February 2024 (and remains blocked), causing disruptions for 16 days in May 2024. 169 of these FQDNs also used the same IP for mail and web hosting. Upon additional investigation, we found out that the IP had been rented by a legitimate Portuguese hosting provider, which we contacted. They confirmed that they noticed the disruption after losing email connectivity with Italian customers. After realizing the issue, they requested a replacement IP from Hetzner, unaware that the previous IP was blocked by Piracy Shield.

Once again, we argue that cases like these demonstrate how IP-level blocking can have far-reaching consequences for unrelated users of the Internet, causing business disruptions that may last for several days. Overall, we found that, on average, domains affected by collateral damage from Piracy Shield remained impacted for approximately 320 days.

As in the previous analysis, we manually classified the web pages of the 7,742 FQDNs affected in the past to determine their nature. Among these, 2,220 were still responding to HTTP(S) requests. Of those, we identified 665 as non–streaming-related, 411 as involved in streaming activity, and for 1,114 we were again unable to determine the category due to reasons such as parked domains, access restrictions, or incomplete content. Looking at the language distribution of the non–streaming-related domains, we found that, contrary to the active collateral blocking cases, the vast majority (Table VI) were Portuguese. This result can likely be explained by the incident involving the Portuguese hosting provider described earlier. Among the few Italian websites affected by collateral damage, we identified one belonging to an architectural firm.

TABLE VI: Top 10 languages found in past collateral-damaged, confirmed non-streaming FQDNs

Language	Count	Language	Count
Portuguese	245	Swedish	12
English	236	Catalan	8
Spanish	50	Danish	8
French	30	Turkish	7
Indonesian	17	Others	37
German	15	Total	665

As the final part of our analysis, we investigated whether any addresses blocked by Piracy Shield were announced as anycast, using data from [42]. Anycast is often used by on-demand DDoS protection services, and we were interested in whether any blocked addresses were part of such infrastructures. We identified 176 IPs still affected by blocking, spanning 21 /24 anycast prefixes. Among these, we found IPs belonging to StormWall (11), DDoS Guard (1), and X4B (3), three well-known DDoS protection providers. We argue these blocks are particularly concerning, as websites under attack may rapidly migrate to on-demand DDoS protection, potentially resulting in unintended service disruption within Italy.

While analyzing blocked anycast IPs, we found a case of collateral damage involving a Google IP. Closer inspection revealed the IP was used by Telecom Italia to serve a blocking page for FQDNs filtered by Piracy Shield. Although later removed from the blocklist, this case suggests that collateral damage may have affected the blocking infrastructure itself.

D. Evasion

Piracy Shield's blocking mechanism targets only IPv4 and FQDNs, with no evidence of filtering on IPv6, despite IPv6 being fully supported. This creates a potential loophole, allowing illegal streaming operators to use IPv6 to bypass the platform – particularly for users relying on public recursive resolvers, which currently do not apply the FQDNs blocking list. To verify if this tactic is used, we analyzed IPv6 records of 6,630 blocked FQDNs using OpenINTEL historical data. We found that 132 FQDNs (2.0%) already resolved to IPv6 on the block date, while 1,568 (23.6%) started doing so afterward. The remaining 74.4% never resolved to IPv6. While most FQDNs never adopted IPv6, the post-block increase suggests a possibility that some operators may be using it to evade blocking. We also examined the IPv4 addresses associated with each FQDN at the time of blocking. Out 6,630 blocked FQDNs measured by OpenINTEL, 6,406 FQDNs returned an A record, 5,757 (89.9%) had at least one IP in the blocklist, 648 (10.1%) had none, and 254 (4.0%) had a mix of blocked and unblocked IPs, indicating partial overlap. This suggests that some FQDNs may still be reachable via unblocked infrastructure for the aforementioned users. Finally, we investigated whether FQDNs began resolving to new IPv4 addresses after being blocked. Out of 6,630 FQDNs, 5,259 adopted at least one new IP. Among these, 1,220 started to resolve only to an already-blocked IPs, while 4,039 pointed to at least one unlisted IP suggesting again a potential evasion of the blocking mechanism.

[2] For our historical collateral analysis, we considered only IPs and FQDNs that are still blocked today, as the InfoTech website does not provide unblocking dates for previously blocked resources.

V. Discussion

Our results on the collateral damages of IP and FQDN blocking highlight a worrisome scenario, with hundreds of legitimate websites unknowingly affected by blocking, unknown operators experiencing service disruption, and illegal streamers continuing to evade enforcement by exploiting the abundance of address space online, leaving behind unusable and polluted address ranges. Still, our findings represent a conservative lower-bound estimate. Our visibility into the global DNS is not exhaustive, and our damage assessment focused on HTTP(S) availability nowadays, likely missing cascading disruptions on other services like APIs, email, or databases that rely on direct IP connectivity. The platform's impact is multifaceted: *economically*, it disrupts legitimate businesses, from the Italian mechanics to international hosting providers who lose connectivity with their customers; *technically*, it risks systemic failure by blocking shared infrastructure like CDNs and DDoS protectors while polluting the IP address space for future, unsuspecting users; *operationally* it imposes a growing, uncompensated burden on Italian ISPs forced to implement an expanding list of permanent blocks.

A. Operational Consideration for AGCOM

In this scenario, we urge AGCOM and Italian policymakers to critically reassess the current blocking framework. We argue that while FQDN-based blocking may serve as a temporary patch, it should only be applied as a last resort in tightly constrained time windows, i.e., only for the duration of the live event. The evidence of widespread and difficult-to-predict collateral damage suggests that IP-level blocking is an indiscriminate tool with consequences that outweigh its benefits and should not be used. Instead, AGCOM and copyright holders should prioritize legal pathways to pursue the majority of illegal streamers, many of whom operate within the European Union. To mitigate damages, resource owners must be immediately notified when their assets are blocked, and a clear, fast unblocking mechanism must be in place. This could also contribute to curbing abuse: hosting providers, once informed, may try to trace the infringing activity and prevent further misuse. Finally, we argue that the authority should publish the list of blocked resources immediately after enforcement, enabling third parties to vet the action and ensuring a responsive task force can promptly address unintended disruptions.

B. Operational Consideration for Hosters and IP Brokers

In case of publication of such a list, hosters should subscribe to it and constantly monitor their internal resources to curb down abusers, by tracking their evasion across multiple infrastructures and promptly blocking abused resources and communicating to the authority their cleaning as soon as possible, to release those blocks. They should report to their national authority these behaviours to enable large-scale investigation on the *follow-the-money* principle. Similarly, IP brokers could collaborate with authorities and hosters to ensure that they can provide clean address space to new customers.

C. Concerns for National Security

While we agree on the principle of combating illegal streaming, we also see the platform as a potential unintended major threat to national security. The possibility that a hostile actor may obtain access to the platform and issue a blocking request targeting critical nationwide infrastructure represents a serious risk that both the government and the authority should carefully evaluate. While having an allow list of IPs and FQDNs is a good starting point, policymakers should be aware that third-party dependencies of critical services are often extremely difficult to fully map, and even their operators may lack a complete view of their own dependency chains [43]–[45]. We argue that concentrating control over critical aspects of Italy's Internet infrastructure in a single, opaque platform – without a formal mechanism for ISPs to challenge or appeal its decisions – creates a systemic risk that may ultimately outweigh the benefits of combating online abuse.

D. Ethics

While validating the leaked list of blocked resources, measuring FQDNs, and classifying websites, we adopted low probing rates to avoid burdening the target infrastructures. We did not mention the names of end-user companies, IP addresses, or FQDNs affected by the blocking, to prevent unintended reputational harm. All measurements were conducted from outside Italy to ensure compliance with national laws prohibiting access to blocked content. After careful consideration, we chose not to publicly release the validated list to avoid becoming the primary distributor, but we urge AGCOM to make this data available to enable further research.

VI. Conclusion

In this work, we shed light for the first time on the Italian anti-piracy platform Piracy Shield. We investigated the unintended consequences of IP and FQDN blocking, showing that hundreds of websites suffer or have suffered collateral damages from blocking actions in Italy caused by the platform. This occurs while illegal streamers still manage to evade enforcement by continuously changing their entry points. Our analysis required a significant amount of manual effort, from the reconstruction of the blocked list of resources, which has never been made public by AGCOM, to the classification of the affected domains. As a natural future direction, we see the need for a more longitudinal and live observation of the platform's blocking activity, together with the development of more accurate mechanisms for automatic content classification to better distinguish legitimate services from illegal streaming activities. To conclude, we hope that this work sparks a thorough discussion among Italian operators, AGCOM, and national policymakers on reconsidering the Piracy Shield initiative. This reflection must account for the significant collateral damage to legitimate infrastructure and the potential threat to national security the platform may pose. Ultimately, the challenge is not whether piracy should be fought, but how to do so without endangering the very principles and infrastructure that sustain the Internet as we know nowadays.

Acknowledgments

We thank Gustavas Davidavicius and Vincentas Grinius from IPXO for their insightful analysis of leasing address space. We are also grateful to Massimiliano Stucchi and the ITNOG and RIPE communities for the fruitful discussions that inspired this paper. Our thanks extend to Ben Du, Bernhard Degen, Etienne Khan, and Roland van Rijswijk-Deij for their support and valuable insights.

References

[1] G. Rodríguez, “Countering Piracy,” https://the-marketinghub.com/sportian/docs/240409-Sportian-Case-Study-LALIGA-Content-Protection.pdf, 2024.

[2] G. Radauskas, “Spain’s fight against La Liga streaming pirates hurts thousands of innocent sites,” https://cybernews.com/news/spain-laliga-streaming-piracy-campaign/.

[3] E. van der Sar, “France Escalates War on Sports Piracy with Real-Time IP Blocking,” https://torrentfreak.com/france-escalates-war-on-sports-piracy-with-real-time-ip-blocking/.

[4] AGCOM, “Piattaforma Piracy Shield,” https://www.agcom.it/competenze/antipirateria-e-piracy-shield/piattaforma-piracy-shield, 2025.

[5] F. D. Giorgi, “Piracy is counted out: new Italian Law to fight copyright infringements on electronic communications networks,” https://merlin.obs.coe.int/article/9851, 2023.

[6] R. Barnes, A. Cooper, O. Kolkman, D. Thaler, and E. Nordmark, “Technical Considerations for Internet Service Blocking and Filtering,” RFC 7754, Mar. 2016.

[7] M. Ansar, A. Sperotto, and R. Holz, “Web Crawl Refusals: Insights From Common Crawl,” in *Passive and Active Measurement Conference (PAM 2025)*, Mar. 2025.

[8] M. Liberato, A. Affinito, B. Meijring, M. Jonker, A. Botta, and A. Sperotto, “To Block Or Not To Block? Evaluating Parental Controls Across Routers, DNS Services, and Software,” in *9th Network Traffic Measurement and Analysis Conference*, 2025.

[9] L. Deri and F. Fusco, “Evaluating IP Blacklists Effectiveness,” in *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2023.

[10] A. Master and C. Garman, “A worldwide view of nation-state internet censorship,” *Free and Open Communications on the Internet*, 2023.

[11] D. Xue, B. Mixon-Baca, ValdikSS, A. Ablove, B. Kujath, J. R. Crandall, and R. Ensafi, “TSPU: Russia’s decentralized censorship system,” in *Proceedings of the ACM Internet Measurement Conference*, 2022.

[12] R. S. Raman, L. Evdokimov, E. Wurstrow, J. A. Halderman, and R. Ensafi, “Investigating Large Scale HTTPS Interception in Kazakhstan,” in *Proceedings of the ACM Internet Measurement Conference*, 2020.

[13] N. P. Hoang, J. Dalek, M. Crete-Nishihata, N. Christin, V. Yegneswaran, M. Polychronakis, and N. Feamster, “GFWeb: Measuring the great firewall’s web censorship at scale,” in *33rd USENIX Security Symposium*, 2024.

[14] M. Liu, Y. Zhang, X. Li, C. Lu, B. Liu, H. Duan, and X. Zheng, “Understanding the implementation and security implications of protective DNS services,” in *Proceedings of 2024 Network and Distributed System Security Symposium*, 2024.

[15] InternetNZ, “To block or not to block - Technical and policy considerations of Internet filtering,” https://internetnz.nz/assets/Archives/Content_Blocking_InternetNZ.pdf, 2025.

[16] ICANN Security and Stability Advisory Committee, “DNS Blocking Revisited,” ICANN, SSAC Report SAC127, 2025.

[17] Interpol, “Digital Piracy,” https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Digital-piracy.

[18] P. Monitor, “France: ARCOM reports illegal sports site & domain blocking for 2022-2024 and 2025 through April,” https://piracymonitor.org/france-arcom-reports-illegal-sports-site-domain-blocking-for-2022-2024-and-2025-through-april/.

[19] J. Poort, J. Leenheer, J. van der Ham, and C. Dumitru, “Baywatch - Two approaches to measure the effects of blocking access to The Pirate Bay,” *Telecommunications Policy*, 2014.

[20] M. Stucchi, “Blocking and censoring the italian internet for football reasons: An explanation and history,” https://ripe89.ripe.net/presentations/114-10-RIPE89-PiracyShield.pdf, 2024.

[21] A. Maxwell, “Italy Approves Piracy Shield VPN/DNS Proposal, Risk of Prison for ISPs Intact,” https://torrentfreak.com/italy-approves-piracy-shield-vpn-dns-proposal-risk-of-prison-for-isps-intact-241001/, 2024.

[22] ——, “Google Receives Piracy Shield Orders to Block Pirate Sites in Public DNS,” https://torrentfreak.com/google-receives-piracy-shield-orders-to-block-pirate-sites-in-public-dns-250618/, 2025.

[23] B. Zawrzel, “Stavolta Piracy Shield l’ha fatta grossa e ha bloccato Google Drive,” https://www.wired.it/article/piracy-shield-blocco-google-drive-download/, 2024.

[24] I. Post, “La piattaforma nazionale anti pirateria ha bloccato Google Drive per errore,” https://www.ilpost.it/2024/10/20/google-drive-bloccato-anti-pirateria/, 2024.

[25] M. Follis, “L’autogol di Piracy Shield, così la piattaforma anti-pezzotto di Agcom ha bloccato per errore dei servizi di Google,” https://www.lastampa.it/sport/2024/10/20/news/piracy_shield_agcom_blocca_google_drive-14734331/, 2024.

[26] M. Masnick, “Italy’s Piracy Shield Misfires, Blocks Google Drive In Anti-Piracy Blunder,” https://www.techdirt.com/2024/10/21/italys-piracy-shield-misfires-blocks-google-drive-in-anti-piracy-blunder/, 2024.

[27] G. Moody, “Massive Expansion of Italy’s Piracy Shield Underway Despite Growing Criticism of Its Flaws,” https://walledculture.org/massive-expansion-of-italys-piracy-shield-underway-despite-growing-criticism-of-its-flaws/, 2025.

[28] E. Commission, “Notification 2025/0148/IT,” https://torrentfreak.com/images/EC-comments-to-Italy-Addressing-Concerns-250613-.pdf, 2025.

[29] Techdirt, “Massive Expansion Of Italy’s Piracy Shield Underway despite growing criticism of its flaws,” https://www.techdirt.com/2025/04/03/massive-expansion-of-italys-piracy-shield-underway-despite-growing-criticism-of-its-flaws/, 2025.

[30] EuroISPA, “Piracy Shield: A flawed approach in the fight against online piracy,” https://www.euroispa.org/2025/04/piracy-shield-a-flawed-approach-in-the-fight-against-online-piracy/, Apr. 2025.

[31] A. Maxwell, “Piracy Shield Crisis Erupts as AGCOM Board Member Slams Huge Toll on Resources,” https://torrentfreak.com/piracy-shield-crisis-erupts-agcom-board-member-slams-huge-toll-on-resources-241103/, 2024.

[32] ——, “Piracy Shield Fails to Convert Pirates to Paying Subscribers, Data Suggests,” https://torrentfreak.com/piracy-shield-fails-to-convert-pirates-to-paying-subscribers-data-suggest-250119/, 2025.

[33] AGCOM, “Blocchi IPs,” https://blocchips.agcom.it/, 2025.

[34] Infotech S.r.l., “Piracy Shield Search,” https://piracyshield.iperv.it/, 2025.

[35] Anonymous, “Leaked List,” https://github.com/PiracyShield/RoutingTable, 2025.

[36] B. Du, R. Fontugne, C. Testart, A. C. Snoeren, and k. claffy, “Sublet Your Subnet: Inferring IP Leasing in the Wild,” in *Proceedings of the ACM Internet Measurement Conference*, 2024.

[37] B. Degen, B. Du, R. K. P. Mok, R. Sommese, M. Jonker, R. van Rijswijk-Deij, and kc claffy, “From Scarcity to Opportunity: Examining Abuse of the IPv4 Leasing Market,” in *9th Network Traffic Measurement and Analysis Conference*, Jun. 2025.

[38] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras, “A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements,” *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 6, 2016.

[39] R. Sommese, R. van Rijswijk-Deij, and M. Jonker, “This Is a Local Domain: On Amassing Country-Code Top-Level Domains from Public Data,” *SIGCOMM Comput. Commun. Rev.*, vol. 54, no. 2, 2024.

[40] Google, “List of all known and announced CT Logs,” https://www.gstatic.com/ct/log_list/v3/all_logs_list.json, 2025.

[41] IPinfo, “IPinfo Lite,” https://ipinfo.io/lite, 2025.

[42] R. Hendriks, M. Luckie, M. Jonker, R. Sommese, and R. van Rijswijk-Deij, “LACeS: an Open, Fast, Responsible and Efficient Longitudinal Anycast Census System,” in *Proceedings of the ACM Internet Measurement Conference*, 2025.

[43] R. Sommese, M. Jonker, J. van der Ham, and G. Moura, “Assessing e-Government DNS Resilience,” in *18th International Conference on Network and Service Management*, Oct. 2022.

[44] R. Kumar, E. Carisimo, L. D. A. Riva, M. Buzzone, F. E. Bustamante, I. A. Qazi, and M. G. Beiró, “Of Choices and Control - A Comparative Analysis of Government Hosting,” in *Proceedings of the ACM Internet Measurement Conference*, 2024.

[45] A. Kashaf, V. Sekar, and Y. Agarwal, “Analyzing Third Party Service Dependencies in Modern Web Services: Have We Learned from the Mirai-Dyn Incident?” in *Proceedings of the ACM Internet Measurement Conference*, 2020.