

1 Understanding Partial Reachability in the Internet 2 Core

3 **Guillermo Baltra**  

4 USC/ISI, Marina del Rey, California, USA

5 **Tarang Saluja** 

6 Swarthmore College, Swarthmore, Pennsylvania, USA

7 **Yuri Pradkin**  

8 USC/ISI, Marina del Rey, California, USA

9 **John Heidemann**  

10 USC/ISI, Marina del Rey, California, USA

11 — Abstract

12 Routing strives to connect all the Internet, but compete: political pressure threatens routing
13 fragmentation; architectural changes such as private clouds, carrier-grade NAT, and firewalls make
14 connectivity conditional; and commercial disputes create partial reachability for days or years. This
15 paper suggests *persistent, partial reachability is fundamental to the Internet* and an underexplored
16 problem. We first *derive a conceptual definition of the Internet core* based on connectivity, not
17 authority. We identify *peninsulas*: persistent, partial connectivity; and *islands*: when computers
18 are partitioned from the Internet core. Second, we develop algorithms to observe each across the
19 Internet, and apply them to two existing measurement systems: Trinocular, where 6 locations
20 observe 5M networks frequently, and RIPE Atlas, where 13k locations scan the DNS roots frequently.
21 Cross-validation shows our findings are stable over *three years of data*, and consistent with as few
22 as 3 geographically-distributed observers. We validate peninsulas and islands against CAIDA Ark,
23 showing good recall (0.94) and bounding precision between 0.42 and 0.82. Finally, our work has
24 broad practical impact: we show that *peninsulas are more common than Internet outages*. Factoring
25 out peninsulas and islands as noise can *improve existing measurement systems*; their “noise” is 5×
26 to 9.7× larger than the operational events in RIPE’s DNSmon. We show that most peninsula events
27 are routing transients (45%), but most peninsula-time (90%) is due to a few (7%) long-lived events.
28 Our work helps inform Internet policy and governance, with our neutral definition showing no single
29 country or organization can unilaterally control the Internet core.

30 **2012 ACM Subject Classification** Networks → Network measurement; Networks → Public Internet;
31 Networks → Network economics

32 **Keywords and phrases** Internet, Internet reliability, Network outages, Active measurements

33 **Digital Object Identifier** [10.4230/OASIcs.NINeS.2026.4](https://doi.org/10.4230/OASIcs.NINeS.2026.4)

34 **Related Version** *Full Version:* <http://arxiv.org/abs/2601.12196>

35 **Funding** The work is supported in part by the National Science Foundation, CISE Directorate,
36 award CNS-2007106 NSF-2028279, OAC-2530698, and DARPA Contract HR001124C0403. Any
37 opinions, findings and conclusions or recommendations expressed in this material are those of the
38 author(s) and do not necessarily reflect the views of NSF or DARPA. The U.S. Government is
39 authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any
40 copyright notation thereon.

41 **Acknowledgements** The authors would like to thank John Wroclawski, Wes Hardaker, Ramakrishna
42 Padmanabhan, Ramesh Govindan, Eddie Kohler, and the Internet Architecture Board for their input
43 on an early version of this paper. We would also like to thank the NINeS chairs and steering
44 committee for building a venue that is receptive for this kind of paper, and to our shepherd, Michael
45 Schapira, and the reviewers for their input.



© Guillermo Baltra, Tarang Saluja, Yuri Pradkin, John Heidemann;
licensed under Creative Commons License CC-BY 4.0

1st New Ideas in Networked Systems (NINeS 2026).

Editors: Katerina J. Argyraki and Aurojit Panda; Article No. 4; pp. 4:1–4:31



OpenAccess Series in Informatics

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

46 **1** Introduction

47 The Internet was created to allow disparate networks to communicate [18, 73, 20], making
 48 *network partition* its nemesis. Routing is designed to heal partitions, so that “communication
 49 must continue despite loss of networks or gateways” [20]. Yet the reality of partitions prompts
 50 leadership-election algorithms such as Paxos [60].

51 Worse than complete network partition is *long-lived partial reachability*. Although transient
 52 reachability problems are well known (for example, [100]), and human errors occur [64],
 53 *policy choices* can cause persistent partial connectivity. Economic differences result in
 54 peering disputes [67, 76, 42]; while political choices can limit access [80], or emphasize
 55 sovereignty [71, 26, 79]. Research [2, 57, 58] and production [89, 102] work around persistent
 56 unreachability.

57 **Challenges:** But today *universal reachability in the Internet core is often challenged*:
 58 *Political* pressure may Balkanize the Internet along national borders. Examples include
 59 Russia’s 2019 sovereign-Internet law [71, 26, 79] and national “Internet kill switches” that are
 60 debated in U.S. [46] and the U.K., and deployed elsewhere [25, 23, 48, 93]. These pressures
 61 prompted policy discussions about fragmentation [33, 34]. We suggest that *technical methods*
 62 *can help inform policy discussions* and that threats such as de-peering place the global
 63 Internet at risk. We will show that no single country can unilaterally control the Internet
 64 core today (§6.2), and that de-peering *can* fragment the Internet core into pieces (§6.1).

65 *Architecturally*, 25 years of evolution have segmented the Internet core: many services live
 66 in clouds; users are usually second-class clients due to Network Address Translation (NAT);
 67 firewalls interrupt connectivity; and Internet has both IPv4 and IPv6. Politics can influence
 68 architecture, with China’s Great Firewall [4, 5], and a proposed “new Internet” [39]. We
 69 suggest that technical methods help us *reason about changes to Internet architecture*, to
 70 understand implications of partial reachability and evaluate IPv6 deployment.

71 *Operationally*, even when ISP peering is mature, disputes can cause long-term partial
 72 unreachability [67]. Such unreachability detected experimentally [31], and systems built
 73 to mitigate partial reachability [2, 57, 58]. We show several operational uses of our work.
 74 We show that *accounting for partial reachability can make existing measurement systems*
 75 *more sensitive*. By applying these results to widely used RIPE DNSmon (§6.3), we show
 76 that its observations of persistent high query loss (5–8% to the DNS Root [85]) are mostly
 77 measurement error and persistent partial connectivity. These factors are 5× and 9.7×
 78 (IPv4 and v6) larger than operationally important signals. Our analysis also helps resolve
 79 uncertainty in Internet outage detection (§6.2), clarifying “corner cases” due to conflicting
 80 observations [90, 75, 91, 81, 49]. We show partial reachability is a common cause, and it
 81 occurs at least as often as complete outages (§5.1). Finally, our work helps quantify the
 82 applicability of route-failure mitigation [2, 57, 58], and of cloud egress selection [89].

83 **Contributions:** Our first contribution is to *recognize that partial reachability is a*
 84 *fundamental part of the Internet*, and addressing it requires a *rigorous definition of what*
 85 *is the Internet’s core* (§2). In 1982, the Internet was 83 hosts [92] globally reachable with
 86 TCP/IP [73]. In 1995, the Federal Networking Council defined “Internet” as (i) a global
 87 address space, (ii) supporting TCP/IP and its follow-ons, that (iii) provides services [41].
 88 Later work added DNS [56] and IPv6. But today’s Internet is much changed: Both users
 89 on PCs and the majority of users on mobile devices access the Internet indirectly through
 90 NAT [96] and Carrier-Grade NAT (CG-NAT) [82]. Many public services operate from the
 91 cloud, visible through rented or imported IP addresses, backed by network virtualization [47].
 92 Media is replicated in Content Delivery Networks (CDNs). Access is mediated by firewalls.

data source	num. VPs	measurement		
		freq.	targets	duration
Trinocular [75]	6 ^a	11 min.	5M /24s	4 years
RIPE Atlas [83]	12,086 ^b	5 min.	13 RSOs	3 years
CAIDA Ark [14]	171 ^c	24 hrs.	all IPv4	selected
Routeviews [65]	55 ^d	1 hour	all IPv4	selected

a: In 2017 and 2019. b: On 2024-01-30. c: On 2017-12-01. d: In 2024-01.

Table 1 Types of data sources used in this paper.

93 Yet users find Internet services so seamless that technology recedes and the web, Facebook,
94 and phone apps are their “Internet”.

95 *We define Internet core as the strongly-connected component of more than 50% of active,
96 public IP addresses that can bidirectionally route to each other (§2.1).* This definition
97 has several unique characteristics. First, captures the uniform, *peer-to-peer nature of the*
98 *Internet core* necessary for first-class services. Second, it defines *one, unique* Internet core by
99 requiring reachability of more than 50%—there can be only one since multiple majorities are
100 impossible. Finally, unlike prior work, this *conceptual* definition avoids dependence on any
101 specific measurement system, nor does it depend on historical precedent, special locations,
102 or central authorities. Although an operational measurements will reflect observation error,
103 the conceptual Internet core defines an asymptote against which our current and future
104 measurements can compare, unlike prior definitions from specific systems [2, 57, 58].

105 Our second contribution is to use this definition to identify two classes of persistent
106 *unreachability* (§2.3), and develop algorithms to quantify each (§3). We define *peninsulas* as
107 when a network sees persistent, partial connectivity to part of Internet core. We present the
108 *Taitao* algorithm to detect peninsulas that often result from peering disputes or long-term
109 firewalls. We define *islands* as when one or more computers are partitioned from the main
110 Internet core as detected by *Chiloe*, our second algorithm.

111 We apply these algorithms to data from two operational systems (Table 1): Trinocular,
112 with frequent measurements of 5M networks from six Vantage Points (VPs) [75], and RIPE
113 Atlas, with frequent measurements of the DNS root [85] from 13k VPs [83]. By applying new
114 algorithms to existing, publicly available, multi-year data we are able to provide longitudinal
115 analysis with some results covering more than three years. These two systems demonstrate
116 our approach works on active probes covering millions of networks (although from few
117 observers) and also from more than 13k VPs (although probing only limited destinations),
118 strongly suggesting the results generalize, since no practical system can cover the $O(n^2)$ cost
119 of all destinations from all sources.

120 In addition varying VPs and destinations across the design space, we evaluate the
121 accuracy of our systems with rigorous measurements (§4). We quantify the independence of
122 the Trinocular sites (§4.3) with cross-validation. Our analysis shows that combinations of
123 any three independent VPs provide a result that is statistically indistinguishable from the
124 asymptote §5.1. We show our results are stable over more than three years with samples from
125 Trinocular (§4.2) and continuous results from RIPE Atlas (§6.3). Finally, we validate both
126 algorithms against a third measurement system, CAIDA Archipelago, where 171 VPs scan
127 millions of networks, daily [13]. Although comparing very different systems is challenging,
128 these results provide strong bounds on accuracy (§4.1), with very good recall (0.94) and
129 reasonable precision (lower and upper bounds from 0.42 and to 0.82).

130 Our final contribution *uses these algorithms to address current operational questions*. We

4:4 Understanding Partial Reachability in the Internet Core

131 show that partial reachability is a *pervasive problem* today, meriting attention. We prove that
132 peninsulas occur *more* often than outages, as subject of wide attention [90, 29, 75, 91, 28, 99].
133 We bring technical light to policy choices around national networks (§6.2) and de-peering
134 (§6.1). We improve sensitivity of RIPE Atlas’ DNSmon [1] (§6.3), resolve corner cases in
135 outage detection (§6.2), and quantify opportunities for route detouring (§5.1).

136 These contributions range from a theoretical definition, to experimental measurements,
137 and their practical application. Each depends on the other—the definition enables the
138 algorithms, which are then applied to show utility.

139 **Artifacts and ethics:** Data used (Table 1) and created [7] in this paper is available at
140 no cost. Our work poses no ethical concerns (§A) by not identifying individuals and avoiding
141 additional traffic by reanalysis with new algorithms. IRB review says it is non-human subjects
142 research (USC IRB IIR00001648).

143 2 Problem: Partial Reachability

144 Understanding partial reachability requires a rigorous definition of *what* is being reached.
145 We next define the *Internet core* to which we connect, to answer the political, architectural,
146 and operational questions from §1.

147 We suggest a definition must be both *conceptual* and *operational* [35]. Our conceptual
148 definition (§2.1) articulates what the Internet *is and is not*. It provides a goal which our
149 implementation (§3) approximates, and we apply it to improve real-world, operational systems
150 (§6.3). Prior definitions [18, 73, 41] are too vague to operationalize.

151 Second, a definition must give both sufficient *and* necessary conditions to be part of
152 the Internet core. Prior work gave properties the core must have (sufficient conditions, like
153 supporting TCP). We add *necessary* conditions to define when networks *leave* the Internet
154 core (§6.1).

155 2.1 The Internet: A Conceptual Definition

156 We define the Internet core as *all active IP addresses that can Bidirectionally Route to more*
157 *than 50% of the public, Potentially Reachable Internet*. We define these key terms next, and
158 expand their motivation and implications later (§2.2).

159 Two addresses are *Bidirectionally Routable* when each can initiate a connection to the
160 other. In our realization we measure connectivity with either ICMP echo-request or with
161 DNS queries and replies, considering alternatives in §2.2.

162 The *Potentially Reachable Internet* is all IP addresses in a graph-theoretic strongly-
163 connected component, with graph edges defined by Bidirectional Routability. This definition
164 means any node in the set can reach any other, either directly or perhaps through one or
165 more hops.

166 2.2 Motivation for *This* Definition

167 We define the potentially reachable Internet via observation, so it depends only on testable,
168 shared information, and not a central authority such as ICANN. Defining the Potentially
169 Reachable Internet as active addresses also implies that the vast parts of unallocated IPv6
170 do not change our conclusions.

171 **Why both bidirectional routability and potential reachability?** *Bidirectional*
172 *Routability* is connectivity in the networking sense, so each address must have a routing table
173 entry that covers the other, and there must be some BGP-level reachability between them.

¹⁷⁴ *Graph-Theoretic Reachability* shows transitive connectivity, even when disputes mean some
¹⁷⁵ pairs cannot reach each other.

¹⁷⁶ Bidirectional Routability is required to capture the idea of IP routing from prior
¹⁷⁷ definitions [18, 73, 41], where all hosts should be able to communicate directly. It excludes
¹⁷⁸ private, NAT’ed addresses [78], which, although useful clients, require rendezvous protocols
¹⁷⁹ (STUN [86], UPnP [66], or PMP [19]) to partially link to the core, and also non-public cloud
¹⁸⁰ addresses hidden behind load balancers [47]. However, cloud VMs with fully-reachable public
¹⁸¹ addresses are part of the core, including cloud-hosted services using public IP addresses from
¹⁸² the cloud operator or their own (BYOIP).

¹⁸³ Graph-Theoretic Reachability is required to define what “100%” is, so we guarantee one
¹⁸⁴ (or no) Internets by looking for a non-overlapping majority, even in the face of conflicting
¹⁸⁵ claims (§B). The combination of terms help us resolve such conflicts as different peninsulas
¹⁸⁶ sharing a common Internet core (although perhaps requiring relay through a third party).

¹⁸⁷ **Why more than 50%?** We take as an axiom that there should be *one Internet core*
¹⁸⁸ per address space (IPv4 and IPv6), or a reason why that Internet core no longer exists. Thus
¹⁸⁹ we require a definition to unambiguously identify “the” Internet core given conflicting claims;
¹⁹⁰ any larger value is excessive, and anything smaller would allow multiple viable claims. (In
¹⁹¹ practice, Figure 8 we see 98.5–99.5% agreement on the core, so values at the 50% threshold
¹⁹² are unlikely.)

¹⁹³ Requiring a majority of active addresses ensures that there can be only one Internet core,
¹⁹⁴ since any two majorities must overlap. Any smaller fraction could allow two groups to make
¹⁹⁵ valid claims. We discuss how to identify the core in the face of conflicting claims in §B.

¹⁹⁶ The definition of the Internet core should not require a central authority. “Majority”
¹⁹⁷ supports assessment independent of any authority. Any computer to prove it is in the Internet
¹⁹⁸ core by reaching half of active addresses, as defined by multiple, independent, long-term
¹⁹⁹ evaluations [51, 103, 27]. It also avoids identification of “tier-1” ISPs, an imprecise term
²⁰⁰ determined only by private business agreements.

²⁰¹ Finally, a majority defines *an Internet core that can end*: fragmentation occurs should the
²⁰² current Internet core break into three or more disconnected components where none retains
²⁰³ a majority of active addresses. If a large enough organization or group chose to secede, or
²⁰⁴ are expelled, the Internet core could become several no-longer internets (§6.1).

²⁰⁵ **Why all addresses?** In each of IPv4 and IPv6 we consider all addresses equally. Public
²⁰⁶ Internet addresses are global, and the Internet core was intentionally designed without a
²⁰⁷ hierarchy [20]. Consistent with decentralization trends [32], a definition should not create
²⁰⁸ hierarchy, nor designate special addresses by age or importance.

²⁰⁹ These definitions are relatively apolitical and reduce first-mover bias, discussed in §6.1.
²¹⁰ Addresses are an Internet-centric metric, unlike population or countries. Requiring activity
²¹¹ reduces the influence of large allocated, but unused, space, such as in legacy IPv4 /8s and
²¹² new IPv6 allocations.

²¹³ **Reachability, Protocols and Firewalls:** End-to-end reachability avoids difficult
²¹⁴ discovery of router-level topology.

²¹⁵ Our conceptual definition allows different definitions of reachability. Reachability may be
²¹⁶ measured by protocols such as ICMP echo-request (pings), DNS or HTTP queries, or by
²¹⁷ data-plane reachability with BGP. Any specific test will provide an operational realization
²¹⁸ of our conceptual definition. (Measurement must tolerate transient failures, perhaps with
²¹⁹ multiple targets (Trinocular) or retransmissions (Atlas).) §5.1 examines how well using
²²⁰ ICMP-based measures converge, and §6.3 shows DNS stability over years.

²²¹ Firewalls complicate observing reachability and can make it conditional. We accept that

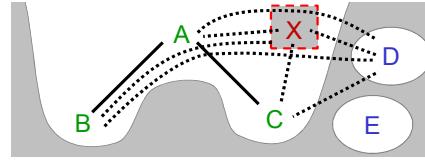


Figure 1 *A, B and C* are the connected core, *B and C* peninsulas, *D and E* islands, *X* is out.

222 the results of specific observations may vary with different protocols or observation times;
 223 experiments show results are stable (§5.1). Measurement allows us to evaluate policy-driven
 224 unreachability (see Appendix G.2 in [9]).

225 We have two implementations of peninsula and island detection; both use publicly-
 226 available data from existing measurement systems. One uses Trinocular [75], because of its
 227 frequent, Internet-wide ICMP echo requests (11-minutes to 5M IPv4 /24s). Prior work has
 228 shown ICMP provides the most response [10, 75, 36], and can avoid rate limiting [50], other
 229 other protocol options are possible. Our second uses RIPE Atlas because of its use in DNS
 230 (§6.3).

231 **Why reachability and not applications?** Users care about applications, and a
 232 user-centric view might emphasize reachability of HTTP or to Facebook rather than at the IP
 233 layer. Our second realization uses public data from RIPE Atlas, with DNS as the application,
 234 as described in §6.3. Many large outages are failures of applications such as DNS [74]; their
 235 study would require a different evaluator than IP reachability. Future work may look at
 236 other, more user-centric applications. However, we suggest reachability at the IP layer is a
 237 more fundamental concept. IP has changed only twice since 1969 with IPv4 and IPv6, but
 238 applications wax and wane, and some (like e-mail) extend beyond the Internet.

239 2.3 Cases of Partial Reachability

240 We use our definition of the Internet core to consider three types of partial reachability,
 241 shown in Figure 1. Here long-term and current routability are dotted and solid lines, and
 242 white regions show current data-plane reachability. All address blocks but *E* form the *core*.
 243 Blocks *B* and *C* are on *peninsulas* because they do not route to each other, although data
 244 could relay through *A*. Block *X* has an *outage*; its routes are temporarily down. Blocks
 245 *D* and *E* are *islands*: *D* usually can route to the core, but not currently. *E* uses public
 246 addresses, but has never announced routes publicly.

247 2.3.1 Outages

248 A number of groups have examined Internet outages [90, 75, 81, 49]. These systems observe
 249 the public IPv4 Internet and identify networks that are no longer reachable—they have left
 250 the Internet. Often these systems define outages operationally (network *X* is out since none
 251 of our VPs can reach it). In this paper, we define an outage as when all computers in a block
 252 are off, perhaps due to power loss. We next define islands, when the computers are on but
 253 cannot reach the Internet core.

254 2.3.2 Islands: Isolated Networks

255 An *island* is a group of public IP addresses partitioned from the Internet core, but still able
 256 to communicate among themselves. Operationally, outages (X in Figure 1) and islands (like

257 D and E) are both unreachable from external VPs and appear identical, but computers in
 258 an island are on and can reach each other.

259 Islands occur when an organization is no longer connected to the Internet core. A business
 260 with one ISP becomes an island when its router upstream connection fails, even though
 261 computers in the business can reach each other. An *address island* is when a computer can
 262 reach only itself.

263 **Example Islands:** Islands are common in RIPE Atlas [1] when a VP has an IPv6
 264 address on the LAN, but lacks routes to the public IPv6 Internet. In §6.3 we show that
 265 this kind of misconfiguration accounts for 5× more IPv6 unreachability than other, more
 266 meaningful problems.

267 We also see islands in reanalysis of data from Trinocular outage detection [75]. Over three
 268 years, from 2017 to 2020, we saw 14 cases where one of the 6 Trinocular VPs was active and
 269 could reach its LAN, but could not reach the rest of the Internet. Network operators confirm
 270 local routing failures in several of these cases. We provide one example in Appendix E.1
 271 of [9].

272 2.3.3 Peninsulas: Partial Connectivity

273 Link and power failures create islands, *peninsulas* are *partial* connectivity, when a group of
 274 public IP addresses can reach some destinations, but not others. (In a geographic peninsula,
 275 the mainland may be visible over water, but reachable only with a detour; similarly, in Figure 1,
 276 *B* can reach *A*, but not *C*.) Peninsulas occur when an upstream provider of a multi-homed
 277 network accepts traffic it cannot deliver or forward, when Tier-1 ISPs refuse to peer, or when
 278 firewalls block traffic. Experimental overlay networks route around peninsulas [2, 57, 58].

279 **Peninsulas in IPv6:** A long-term peninsula follows from the IPv6 peering dispute
 280 between Hurricane Electric (HE) and Cogent. These ISPs decline to peer in IPv6 (IPv4
 281 is fine), nor do they forward their IPv6 through another party. HE and Cogent customers
 282 could not reach each other in 2009 [67], and this problem persists through 2025, as we show
 283 in DNSmon (§6.3). We further confirm unreachability between HE and Cogent users in
 284 IPv6 with traceroutes from looking glasses [38, 24] (HE at 2001:470:20::2 and Cogent at
 285 2001:550:1:a::d): neither can reach their neighbor’s server, but both reach their own. Other
 286 IPv6 disputes include Cogent and Google [76], and Cloudflare and Hurricane Electric [42].
 287 Disputes can arise from an inability to agree to settlement-free or paid peering.

288 **Peninsulas in IPv4:** We observed a peninsula lasting 3 hours starting 2017-10-23t22:02Z,
 289 where five Polish Autonomous Systems (ASes) had 1716 /24 blocks that were always reachable
 290 one Los Angeles, but not from four other VPs (as seen in public data from Trinocular [98]).
 291 Before the peninsula, these blocks received service through Multimedia Polska (MP, AS21021),
 292 via Cogent (AS174), or through Tata (AS6453). When the peninsula occurred, traffic to all
 293 blocks continued through Cogent but was blackholed; it did not shift to Tata. The successful
 294 VP could reach MP through Tata for the entire event, proving MP was connected. After
 295 3 hours, we see a burst of 23k BGP updates and MP is again reachable from all VPs. We
 296 provide additional details in Appendix E.2 of [9].

297 3 Detecting Partial Connectivity

298 We now introduce the *Taitao* algorithm to detect peninsulas, and *Chiloe*, islands (names
 299 from Patagonian geography).

300 **3.1 Taitao: a Peninsula Detector**

301 Peninsulas occur when portions of the Internet core are reachable from some locations and
 302 not others. They can be seen by two VPs disagreeing on reachability.

303 Detecting peninsulas presents three challenges. Without VPs everywhere, when all VPs
 304 are on the same “side” of a peninsula (A and C in Figure 1), their reachability agrees even
 305 though VPs may disagree (like B). Second, asynchronous observations test reachability at
 306 different times: observations in Trinocular spread over 11 minutes, and in Atlas, 5 minutes.
 307 Observations at times before and after a network change will disagree, but both are true—a
 308 difference due to weak synchronization, and not a peninsula. Third, connectivity problems
 309 near the observer (or when an observer is an island) should not reflect on the intended
 310 destination.

311 We identify peninsulas by detecting disagreements in block state by comparing successful
 312 VP observations that occur at about the same time. Since probing rounds occur asynchronously,
 313 we compare measurements within the measurement system’s window (11 or 5 minutes for
 314 Trinocular and Atlas). This approach sees peninsulas lasting longer than one window duration,
 315 but may miss briefer ones, or when VPs are not on “both sides”.

316 Formally, $O_{i,b}$ is the set of observers with valid observations about block b at round i .
 317 We look for disagreements in $O_{i,b}$, defining $O_{i,b}^{up} \subset O_{i,b}$ as the set of observers that measure
 318 block b as up at round i . We detect a peninsula when:

$$319 \quad 0 < |O_{i,b}^{up}| < |O_{i,b}| \quad (1)$$

320 When only one VP reaches a block, we must classify it as a peninsula or an island, as
 321 described next.

322 **3.2 Chiloe: an Island Detector**

323 According §2.3.2, islands occur when the Internet core is partitioned, and the component
 324 with fewer than half the active addresses is the island. Typical islands are much smaller.

325 We can find islands by looking for networks that are only reachable from less than half of
 326 the Internet core. However, to classify such networks as an island and not merely a peninsula,
 327 we need to show that it is partitioned, which requires global knowledge. In addition, if
 328 islands are partitioned from all VPs, we cannot tell an island, with active but disconnected
 329 computers, from an outage, where they are off.

330 For these reasons, we must look for islands that include VPs in their partition. Because
 331 we know the VP is active and scanning we can determine how much of the Internet core is in
 332 its partition, ruling out an outage. We also can confirm the Internet core is not reachable, to
 333 rule out a peninsula.

334 Formally, we say that B is the set of blocks in the Internet core. $B_{i,o}^{up} \subseteq B$ are blocks
 335 reachable from observer o at round i , while $B_{i,o}^{dn} \subseteq B$ is its complement. We detect that
 336 observer o is in an island when it thinks half or more of the observable Internet core is down:

$$337 \quad 0 \leq |B_{i,o}^{up}| < |B_{i,o}^{dn}| \quad (2)$$

338 This method is independent of measurement systems, but is limited to detecting islands
 339 that contain VPs, so *any deployment will certainly undercount islands*. We evaluate islands
 340 in Trinocular and Atlas (§5.5), confirming more VPs see more islands, but that *nearly all*
 341 *reported islands are correct*.

342 Finally, because observations are not instantaneous, we must avoid confusing short-lived
 343 islands with long-lived peninsulas. For islands lasting longer than 11-minutes, we also require
 344 $|B_{i,o}^{up}| \rightarrow 0$. With $|B_{i,o}^{up}| = 0$, it is an address island.

		Ark		
		Conflicting	All Down	All Up
Trinocular	Sites Up	1	20	6
	Conflicting	2	13	5
		3	13	1
		4	26	4
		5	83	13
	Agree	0	6	97
		491,120	90	1,485,394

Table 2 Trinocular and Ark agreement table. Dataset A30, 2017q4.

		Ark	
		Peninsula	Non Peninsula
Taitao	Peninsula	184	251 (strict)
	Non Peninsula	12	1,976,701

Table 3 Taitao confusion matrix. Dataset: A30, 2017q4.

345 3.3 Deployment with Existing Systems

346 We have deployed our algorithms as extensions to two systems: Trinocular and RIPE Atlas.
 347 In both cases, each system provides data to us via existing APIs and we then apply Taitao
 348 and Chiloe and share results back. Processing time for both is modest, with DNSmon running
 349 in minutes and Trinocular taking less time than Trinocular outage detection.

350 For DNSmon, we provide daily outages and peninsulas since 2022-01-01 on a public
 351 website [88]. We have also discussed these results with RIPE and the root operators; RIPE
 352 currently identifies islands manually, and one root operator is using our results to guide
 353 operations. We provide 3.5 years Trinocular analysis at our website [6], and are working
 354 with Trinocular operators to operationalize our algorithms.

355 4 Validating our approach

356 We next validate our algorithms with three data sources.

357 4.1 Can Taitao Detect Peninsulas?

358 We compare Taitao detections from 6 VPs to independent observations taken from more
 359 than 100 VPs in CAIDA’s Ark [14]. This comparison is challenging, because both Taitao and
 360 Ark are imperfect operational systems that differ in probing frequency, targets, and method.
 361 Neither defines perfect ground truth, but agreement suggests likely truth.

362 We believe this complexity is warranted because Ark provides a more diverse perspective
 363 (with 171 locations), if we can account for its much sparser frequency. Ark traceroutes also
 364 allow us to assess *where* peninsulas begin. We expect to see a strong correlation between
 365 Taitao peninsulas and Ark observations. (We considered RIPE Atlas as another external
 366 dataset, but its coverage is sparse, while Ark covers all /24s.)

367 **Identifying comparable blocks:** We study 21 days of Ark observations from 2017-10-10
 368 to -31. Ark covers all networks with two strategies. With team probing in 2017, a 40 VP
 369 “team” traceroutes to all routed /24 about once per day. For prefix probing, about 35 VPs
 370 each traceroute to .1 addresses of all routed /24s every day. We use both types of data:
 371 the three Ark teams and all available prefix probing VPs. We group results by /24 blocks,
 372 considering /24s instead of ASes to be sensitive to intra-AS peninsulas.

373 Ark differs from Taitao’s Trinocular input in three ways: the target is a random address
 374 or the .1 address in each block; it uses traceroute, not ping; and it probes blocks daily, not
 375 every 11 minutes. Sometimes these differences cause Ark traceroutes to fail when a simple
 376 ping succeeds. First, Trinocular’s targets respond more often because it uses a curated
 377 hitlist [40] while Ark does not. Second, Ark’s traceroutes can terminate due to path *loops*
 378 or *gaps* in the path, (in addition to succeeding or reporting target unreachable). We do

4.10 Understanding Partial Reachability in the Internet Core

379 not consider results with gaps, so problems on the path do not bias results for endpoints
380 reachable by direct pings.

381 To correct for differences in target addresses, we must avoid misinterpreting a block as
382 unreachable when the block is online but Ark’s target address is not, we discard traces sent
383 to never-active addresses (those not observed in 3 years of complete IPv4 scans), and blocks
384 for which Ark did not get a single successful response. Since dynamic addressing [72] means
385 Ark often fails with an unreachable last hop, we see conflicting observations in Ark, implying
386 false peninsulas. We therefore trust Ark confirmation of outages and full reachability, but
387 question Ark-only peninsulas.

388 To correct for Ark’s less frequent probing, we compare *long-lived* Trinocular down-events
389 (5 hours or more). Ark measurements are infrequent (once every 24 hours) compared to
390 Trinocular’s 11-minute reports, so short Trinocular events are often unobserved by Ark. (Since
391 outage durations are heavy-tailed, 5 h gives Ark some time to confirm without discarding too
392 many events.) To confirm agreements or conflicting reports from Ark, we require at least 3
393 Ark observations within the peninsula’s span of time. Varying these parameters is potential
394 future work; with small quantitative changes likely, but changes to overall bounds unlikely.

395 We filter out blocks with frequent transient changes or signs of network-level filtering,
396 as prior work [75, 91, 81]. We define the “reliable” blocks suitable for comparison as those
397 responsive for at least 85% of the quarter from each of the 6 Trinocular VPs. (This threshold
398 avoids diurnal blocks or blocks with long outages; values of 90% or less have similar results.)
399 We also discard flaky blocks whose responses are frequently inconsistent across VPs. (We
400 consider more than 10 combinations of VP as frequently inconsistent.) For the 21 days, we
401 find 4M unique Trinocular /24 blocks, and 11M Ark /24 blocks, making 2M blocks in both
402 available for study.

403 **Results:** Table 3 shows outcomes, treating Taitao as prediction and Ark as truth, with
404 details in Table 2. Dark green indicates true positives (TP): when (a) either both Taitao
405 and Ark show mixed results, both indicating a peninsula, or when (b) Taitao indicates a
406 peninsula (1 to 5 sites up but at least one down), Ark shows all-down during the event
407 and up before and after. We treat Ark in case (b) as positive because the infrequency of
408 Ark probing (one probe per team every 24 hours) means we cannot guarantee VPs in the
409 peninsula will probe responsive targets in time. Since peninsulas are not common, so too are
410 true positives, but we see 184 TPs.

411 We show *true negatives* as light green and neither bold nor italic. In almost all of these
412 cases (1.4M) both Taitao and Ark reach the block, agreeing. The vast majority of these
413 are an artifact of our use of Ark as “ground truth”, when it is not designed to accurately
414 measure partitions. The challenge of an Ark claim of peninsula is that about 5/6ths of Ark
415 probes fail in the last hop because it probes a single random address (see [75] figure 6). As a
416 result, while positive Ark results support non-partitions, negative Ark results are most likely
417 a missed target and not an unreachable block; we expand on this analysis in Appendix F.1
418 of [9]. We therefore treat this second most-common result (491k cases) as a true negative.
419 For the same reason, we include the small number (97) of cases where both Ark and Taitao
420 report all-down, assuming Ark terminates at an empty address. We include in this category
421 the 90 events where Ark is all-down and Trinocular is all-up. We attribute Ark’s failure to
422 reach its targets to infrequent probing.

423 We mark *false negatives* as red and bold. For these few cases (only 12), all Trinocular
424 VPs are down, but Ark reports all or some responding. We believe these cases indicate blocks
425 that have chosen to drop Trinocular traffic.

426 Finally, yellow italics shows when Taitao’s peninsulas are *false positives*, since all Ark

		Chiloe		Sites	Events	Per Year
		Island	Peninsula	W	5	1.67
Trinocular	Block Island	2	0	C	11	3.67
	Addr Island	19	8	J	1	0.33
	Peninsula	2	566	G	1	0.33
				E	3	1.00
				N	2	0.67
		All (norm.)		All (norm.)	23	7.67 (1.28)

(a) Chiloe confusion matrix

(b) Detected islands

Table 4 (a) Chiloe confusion matrix, events between 2017-01-04 and 2020-03-31, datasets A28 through A39. (b) Islands detected from 2017q2 to 2020q1.

probes reached the target block. This case occurs when either traffic from some Trinocular VPs is filtered, or all Ark VPs are “inside” the peninsula. Light yellow (strict) shows all the 251 cases that Taitao detects. For most of these cases (201), five Trinocular VPs responding and one does not, suggesting network problems are near one of the Trinocular VPs (since five of six independent VPs have working paths). Discarding these cases we get 40 (orange); still conservative but a *looser* estimate.

The strict scenario sees precision 0.42, recall 0.94, and F_1 score 0.58, and in the loose scenario, precision improves to 0.82 and F_1 score to 0.88. We consider these results a strong lower bound on the size of problem, and confirmation that the peninsulas detected by Taitao are correct.

Of course custom measurement could align with our analysis and should close this bound, but the need to build in long-term, existing data, motivates these early, rough bounds. We expect future work to tighten these bounds.

4.2 Can Chiloe Detect Islands?

Chiloe (§3.2) detects islands when a VP within the island can reach less than half the rest of the world.

Trinocular: To validate Chiloe’s correctness, we compare when a single VP believes to be in an island, against what the rest of the world believes about that VP. We begin with Trinocular, where we have strong evidence for a few VPs, then we summarize Atlas with 13k VPs.

Islands are unreachable, like D in Figure 1. We measure blocks, so if any address in block D can reach another, it is an island. If no external VPs can reach D ’s block, Chiloe confirms an island, but some VP reaching D ’s block implies a peninsula. In §4.3 we show that Trinocular VPs are independent, and therefore no two VPs live within the same island. We believe this definition is the best possible ground truth, since perfect classification requires instant, global knowledge and cannot be measured in practice.

We take 3 years worth of data from all six Trinocular VPs. From Trinocular’s pacing, we analyze 11-minute bins.

In Table 4a we show that Chiloe detects 23 islands across three years. In 2 of these events, the block is unreachable from other VPs, confirming the island with our validation methodology. Manual inspection confirms that the remaining 19 events are islands too, but at the address level—the VP was unable to reach anything but did not lose power, and other addresses in its block were reachable from VPs at other locations. These observations suggest a VP-specific problem making it an island. Finally, for 2 events, the prober’s block was reachable during the event by every site including the prober itself which suggests partial connectivity (a peninsula), and therefore a false positive.

	C	J	G	E	N	IPv4 Addresses			IPv6 Addresses			
						RIR	Active	Allocated	RIR	Allocated	Allocated	
W	0.017	0.031	0.019	0.035	0.020	AFRINIC	15M	2%	121M	3.3%	9,661	3%
C		0.077	0.143	0.067	0.049	APNIC	223M	33%	892M	24.0%	88,614	27.8%
J			0.044	0.036	0.046	China	112M	17%	345M	9.3%	54,849	17.2%
G				0.050	0.100	ARIN	150M	22%	1,673M	45.2%	56,172	17.6%
E					0.058	U.S.	140M	21%	1,617M	43.7%	55,026	17.3%
						LACNIC	82M	12%	191M	5.2%	15,298	4.8%
						RIPE NCC	206M	30%	826M	22.3%	148,881	46.7%
						Germany	40M	6%	124M	3.3%	22,075	6.9%
						Total	676M	100%	3,703M	100%	318,626	100%

Table 5 Similarities all VPs.
Dataset: A30, 2017q4.

Table 6 RIR IPv4 hosts and IPv6 /32 allocation [53, 54].

463 In the 566 non-island events (true negatives), a single VP cannot reach more than 5%
 464 but less than 50% of the Internet core. In each of these cases, one or more other VPs were
 465 able to reach the affected VP’s block, showing they were not an island (although perhaps
 466 a peninsula). The table omits the frequent events when less than 5% of the network is
 467 unavailable from the VP, although they too are true negatives.

468 Bold red shows 8 false negatives. These are events that last about 2 Trinocular rounds or
 469 less (22 min), often not enough time for Trinocular to change its belief on block state.

470 **Atlas:** With 13k VPs, RIPE Atlas provides a broader view of islands. We find 188 (v4)
 471 and 388 (v6) Atlas VPs are islands (§6.3), accounting for *the majority of DNS unreachable*
 472 events. RIPE operators confirmed these are often misconfigurations.

473 **Operators:** Beyond this quantitative comparison, we discussed islands with Trinocular
 474 and RIPE Atlas operators. They confirm our examples and trends (Figure 7).

4.3 Are the Sites Independent?

476 Our evaluation assumes VPs do not share common network paths. VPs improve path diversity
 477 by network diversity and physical distance, particularly with today’s “flatter” Internet [59].
 478 We next quantify and validate this assumption.

479 We measure similarity of observations between pairs of VPs. We examine only cases
 480 where one of the pair disagrees with some other VP, since when all agree, we have no new
 481 information. If the pair agrees with each other, but not with the majority, the pair shows
 482 similarity. If they disagree with each other, they are dissimilar. We quantify similarity S_P
 483 for a pair of sites P as $S_P = (P_1 + P_0)/(P_1 + P_0 + D_*)$, where P_s indicates the pair agrees
 484 on the network having state s of up (1) or down (0) and disagrees with the others, and for
 485 D_* , the pair disagrees with each other. S_P ranges from 1, where the pair always agrees, to 0,
 486 where they always disagree.

487 Table 5 shows similarities for each pair of the 6 Trinocular VPs (as half of the symmetric
 488 matrix). No two sites have a similarity more than 0.14, and most pairs are under 0.08. This
 489 result shows that no two sites are particularly correlated.

4.4 Stability Across Time

491 We confirm our results are not time-dependent by repeating key results in multiple years,
 492 including operational result from 2022 to 2025 (Figure 7 in §6.3), and confirm all results with
 493 multiple sources and dates (see Appendix F.2 of [9]). We expect these results to apply today
 494 since partial reachability has persisted since 2001 [2], with some events lasting years [42], as
 495 our results document (Figure 7). We use older data in some examples to avoid limitations

496 of measurement deployments. During 2017q4, Trinocular had six active VPs and Ark had
 497 three teams, providing strong statements from many perspectives. Trinocular had fewer VPs
 498 in 2019 and early 2020, and Ark has fewer teams today, but 2020 gives quantitatively similar
 499 results (see Appendix F.2 of [9]). §5.4 uses 2020q3 data because Ark observed a very large
 500 number of loops in 2017q4.

501 4.5 Varying Parameters and Geography

502 Our algorithms are influenced by the parameters in our data sources, including how often
 503 and where they probe, where they are placed, and how many VPs they employ, and how
 504 much data we analyze. We vary *all of these parameters* across our datasets (see Table 1),
 505 but the requirement for Internet-wide data spanning months and years means we depend
 506 on existing deployed infrastructure. Systematically varying VP frequency and location is
 507 challenging future work.

508 We believe these diverse data sources *confirm our results apply over a range of geographic*
 509 *locations*. We study locations quantitatively in §4.3) and confirm stable results with Atlas
 510 across 3k ASes and 12k locations in §6.3. Thus, while we certainly greatly *undercount* the
 511 absolute numbers of peninsulas and islands observed from Trinocular’s 6 locations (§5), Atlas
 512 confirms these trends apply with 12k VPs.

513 **IPv6:** Given data, our algorithms apply to both IPv4 and IPv6. We provide results
 514 for both v4 and v6 with RIPE Atlas and DNSmon (§6.3), and for Internet-wide v4 with
 515 Trinocular. Internet-wide IPv6 results depend on v6 outage detection, an area of active and
 516 future research.

517 5 Internet Islands and Peninsulas

518 We now examine islands and peninsulas in the Internet core.

519 5.1 How Common Are Peninsulas?

520 We estimate how often peninsulas occur in the Internet core in three ways. First, we directly
 521 measure the visibility of peninsulas by summing the duration of peninsulas as seen from
 522 six VPs. Second, we confirm the accuracy of this estimate by evaluating its convergence
 523 as we vary the number of VPs—more VPs show more peninsula-time, but a result that
 524 converges suggests it is approaching the limit. Third, we compare peninsula-time to outage-
 525 time, showing that, in the limit, observers see both for about the same duration. Outages
 526 correspond to service downtime [101], and are a recognized problem in academia and industry.
 527 Our results show that *peninsulas are as common as outages*, suggesting peninsulas are an
 528 important new problem deserving attention.

529 **Peninsula-time:** We estimate the duration an observer can see a peninsula by considering
 530 three types of events: *all up*, *all down*, and *disagreement* between six VPs. Disagreement,
 531 the last case, suggests a peninsula, while agreement (all up or down), suggests no problem or
 532 an outage. We compute peninsula-time by summing the time each target /24 has disagreeing
 533 observations from Trinocular VPs.

534 We have computed peninsula-time by evaluating Taitao over Trinocular data for 2017q4 [97].
 535 Figure 2 shows the distribution of peninsulas measured as a fraction of block-time for an
 536 increasing number of sites. We consider all possible combinations of the six sites.

537 First we examine the data with all 6 VPs (the rightmost points). We see that peninsulas
 538 (the middle, disagreement graph) are visible about 0.00075 of the time. This data suggests

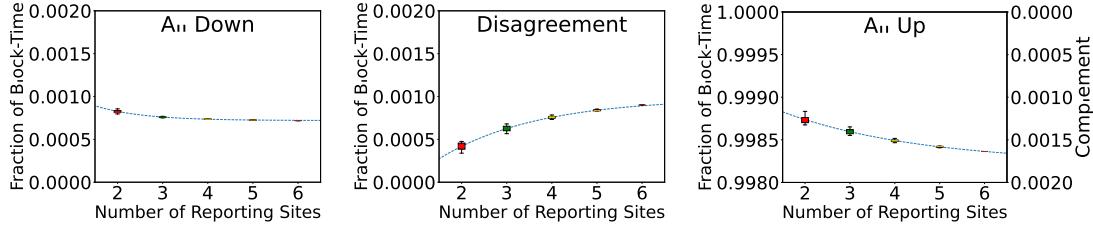


Figure 2 Distribution of block-time fraction: all-down (left), disagreement (center), and all-up (right), events ≥ 1 hour. Data: 3.7M blocks, 2017-10-06 to -11-16, A30.

539 *peninsulas regularly occur, appearing at least 0.075% of the time.* Fortunately, large peninsulas
 540 are rare from many locations—our 6 VPs almost always see the same targets.

541 **Convergence:** While more VPs provide a better view of the Internet core’s overall
 542 state, but the *global fraction* of affected networks will show diminishing returns after major
 543 problems are found. That is previously inferred outages (all unreachable) should have been
 544 peninsulas, with partial reachability. All-down (left) decreases from an average of 0.00082
 545 with 2 VPs to 0.00074 for 6 VPs. All-up (right) goes down a relative 47% from 0.9988 to
 546 0.9984, while disagreements (center) increase from 0.0029 to 0.00045. Outages (left) converge
 547 after 3 sites, as shown by the fitted curve and decreasing variance. Peninsulas and all-up
 548 converge more slowly. We conclude that *a few, independent sites (3 or 4) converge on a good*
 549 *estimate of the fraction of true islands and peninsulas.*

550 We support this claim by comparing all non-overlapping combinations of 3 sites. If all
 551 combinations are equivalent, then a fourth site will not add new information. Six VPs yield
 552 10 possible sets of 3 sites; we examine those combinations for each of 21 quarters, from 2017q2
 553 to 2020q1. When we compare the one-sample Student *t*-test to evaluate if the difference of
 554 each pair of combinations of those 21 quarters is greater than zero, none of the combinations
 555 are rejected at confidence level 99.75%, suggesting that any combination of three sites is
 556 statistically equivalent and confirm our claim that a few sites are sufficient for estimation.

557 **Relative impact:** Finally, comparing outages (the left graph) with peninsulas (the
 558 middle graph), we see both occur about the same fraction of time (around 0.00075). This
 559 comparison shows that *peninsulas are about as common as outages*, suggesting they deserve
 560 more attention.

561 **Generalizing:** We confirm that each of these results holds in a subsequent year in
 562 Appendix F.2 of [9], suggesting the result is not unique to this quarter. While we reach a
 563 slightly different limit (in that case, peninsulas and outages appear about in 0.002 of data),
 564 we still see good convergence after 4 VPs.

565 While this data demonstrates convergence on the *rate* of peninsulas and islands, we
 566 confirm the rate and show a larger absolute *number* of peninsulas with DNSmon’s 12k VPs.

5.2 How Long Do Peninsulas Last?

568 Peninsulas have multiple root causes: some are short-lived routing misconfigurations while
 569 others reflect long-term disagreements in routing policy. In this section we determine the
 570 distribution of peninsulas in terms of their duration to determine the prevalence of persistent
 571 peninsulas. We will show that there are millions of brief peninsulas, likely due to transient
 572 routing problems, but that 90% of peninsula-time is in long-lived events (5 h or more,
 573 following §4.1).

574 We use Taitao to see peninsula duration for all detected in 2017q4: some 23.6M peninsulas

575 affecting 3.8M unique blocks. If instead we look at *long-lived* peninsulas (at least 5 h), we
 576 see 4.5M peninsulas in 338k unique blocks.

577 [Figure 4](#) examines peninsula duration in three ways: a cumulative distribution (CDF)
 578 counting all peninsula events (left, solid, purple line), the CDF of the number of peninsulas
 579 for VP-down events longer than 5 hours (middle, solid green line), and the cumulative size of
 580 peninsulas for VP down events longer than 5 hours (right, green dashes).

581 We see that there are many very brief peninsulas (purple line): about 65% last only
 582 20–60 minutes (~2–6 observations). With two or more observations, these events are not
 583 just one-off measurement loss. These results suggest that while the Internet core is robust,
 584 there are many small connectivity glitches (7.8M events). Events that are two rounds (20
 585 minutes) or shorter may be due to transient BGP blackholes [12].

586 The number of day-long or multi-day peninsulas is small, only 1.7M events (2%, the
 587 purple line). However, about 57% of all peninsula-time is in such longer-lived events (the
 588 right, dashed line), and 20% of time is in events lasting 10 days or more, even when longer
 589 than 5 hours events are less numerous (compare the middle, green line to the left, purple line).
 590 Day-long events persist long enough for human network operators to respond, and events
 591 lasting longer than a week suggest potential policy disputes and *intentional* unreachability.
 592 Together, these long-lived events suggest that there is benefit to identifying non-transient
 593 peninsulas and addressing the underlying routing problem.

594 5.3 What Sizes Are Peninsulas?

595 When network issues cause connectivity problems like peninsulas, the *size* of those problems
 596 may vary, from country-size(see Appendix G.2 in [9]), to AS-size, and also for routable
 597 prefixes or fractions of prefixes. We next examine peninsula sizes.

598 We begin with Taitao peninsula detection at a /24 block level. We match peninsulas
 599 across blocks within the same prefix by start time and duration, both measured in one hour
 600 timebins. This match implies that the Trinocular VPs observing the blocks as up are also
 601 the same.

602 We compare peninsulas to routable prefixes from Routeviews [65], using longest prefix
 603 matches with /24 blocks.

604 Routable prefixes consist of many blocks, some of which may not be measurable. We
 605 therefore define the *peninsula-prefix fraction* for each routed prefix as fraction of blocks in
 606 the peninsula that are Trinocular-measurable blocks. To reduce noise provided by single
 607 block peninsulas, we only consider peninsulas covering 2 or more blocks in a prefix.

608 [Figure 3a](#) shows the number of peninsulas for different prefix lengths and the fraction of
 609 the prefix affected by the peninsula as a heat-map, where we group them into bins.

610 We see that about 10% of peninsulas are likely due to routing problems or policies, since
 611 40k peninsulas affect the whole routable prefix. However, a third of peninsulas (101k, at the
 612 bottom of the plot) affect only a very small fraction of the prefix. These low prefix-fraction
 613 peninsulas suggest that they happen *inside* an ISP and are not due to interdomain routing.

614 Finally, we show that *long-lived peninsulas are likely due to routing or policy choices*.
 615 [Figure 3b](#) shows the same data source, but weighted by fraction of time each peninsula
 616 contributes to the total peninsula time during 2017q4. Here the larger fraction of weight are
 617 peninsulas covering full routable prefixes—20% of all peninsula time during the quarter (see
 618 left margin).

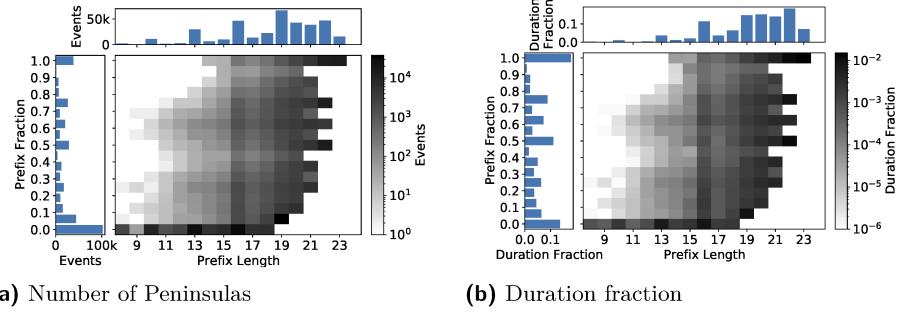


Figure 3 Peninsulas measured with per-site down events longer than 5 hours. Dataset A30, 2017q4.

Sites Up	Target AS		Target Prefix	
	At	Before	At	Before
0	21,765	32,489	1,775	52,479
1	587	1,197	113	1,671
2	2,981	4,199	316	6,864
3	12,709	11,802	2,454	22,057
4	117,377	62,881	31,211	149,047
5	101,516	53,649	27,298	127,867
1-5	235,170	133,728	61,392	307,506
6	967,888	812,430	238,182	1,542,136

Table 7 Halt location of failed traceroutes for peninsulas longer than 5 hours. Dataset A41, 2020q3.

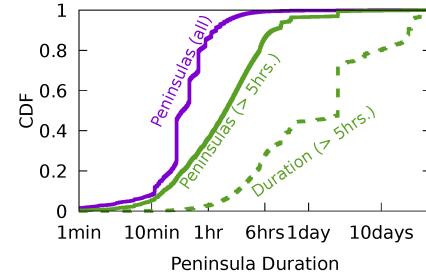


Figure 4 Cumulative peninsulas and peninsula duration. Dataset A30, 2017q4.

5.4 Where Do Peninsulas Occur?

Firewalls, link failures, and routing problems cause peninsulas on the Internet, and can occur at AS boundaries or inside an AS. We next show that *many peninsulas occur at AS boundaries, consistent with policies as a cause* for long-lived events. (Short-lived events at AS boundaries may be routing transients or operator error that is quickly corrected.)

To detect *where* the Internet breaks into peninsulas, we look at traceroutes that failed to reach their target address, either due to a loop or an ICMP unreachable message. Then, we examine if the traceroute halts *at* the target AS and target prefix, or *before* the target AS and prefix.

For our experiment we run Taitao to detect peninsulas at target blocks over Trinocular VPs, we use Ark's traceroutes [15] to find last IP address before halt, and we get target and halting ASNs and prefixes using RouteViews.

In Table 7 we show how many traces halt *at* or *before* the target network. The center, gray rows show peninsulas (disagreement between VPs) with their total sum in bold. For all peninsulas (the bold row), more traceroutes halt at or inside the target AS (235k vs. 134k, the left columns), but they more often terminate before reaching the target prefix (308k vs. 61k, the right columns). (While traceroutes are imperfect, these large differences (2× or more) suggest a robust qualitative conclusion.) This difference suggests policy is implemented at or inside ASes, but not at routable prefixes. By contrast, outages (agreement with 0 sites up) more often terminate before reaching the target AS. Because peninsulas are more often at or in an AS, while outages occur in many places, it suggests that long-lived peninsulas are policy choices consistent with public operator reports [67, 62, 3, 77, 94, 17].

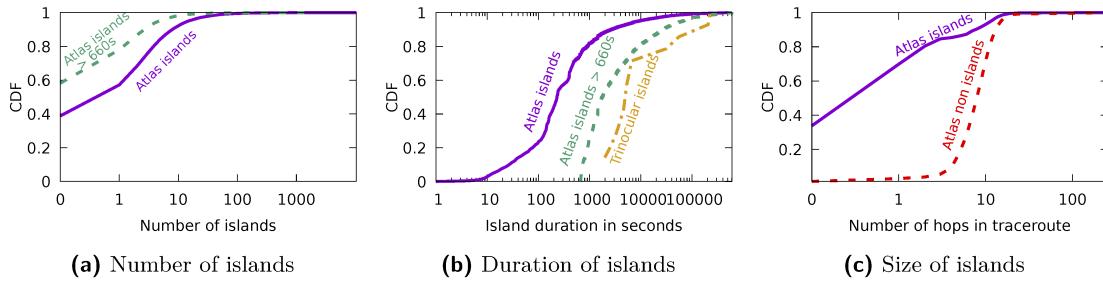


Figure 6 CDF of islands detected by Chiloe for data from Trinocular (3 years, Datasets A28-A39) and Atlas (2021q3).

641 5.5 How Common Are Islands?

642 Multiple groups have shown that there are many network outages in the Internet [90, 75, 91, 643 81, 49]. We have described (§2) two kinds of outages: full outages where all computers at a 644 site are down (perhaps due to a loss of power), and islands, where the site is cut off from the 645 Internet core, but computers at the site can talk between themselves. We next use Chiloe to 646 determine how often islands occur. We study islands in two systems with 6 VPs for 3 years 647 and 13k VPs for 3 months.

648 **Trinocular:** We first consider three years of Trinocular data (Table 1), from 2017-04-01 649 to 2020-04-01. We run Chiloe across each VP for this period.

650 Table 4b shows the number of islands per VP over this period. Over the 3 years, all 651 six VPs see from 1 to 5 islands. In addition, we report as islands some cases even though 652 not the *entire* Internet core is unreachable. This apparent discrepancy from our definition 653 reflects the limitations of our necessarily non-instantaneous measurement of the Internet. We 654 expect such cases, and perhaps other 12 non-islands where 20% to 50% is inaccessible, are 655 *short-lived* true islands, that are incompletely measured because the island recovers before 656 we complete an 11 minute-long evaluation of all 5M networks for a full Internet scan (see 657 §C.2 for details).

658 **RIPE Atlas:** For broader coverage we next consider RIPE Atlas' 13k VPs for all of 659 2021q3 [69]. While Atlas does not scan the whole Internet core, they do scan most root DNS 660 servers every 240s. Chiloe would like to observe the whole Internet core, and while Trinocular 661 scans 5M /24s, it does so with only 6 VPs. To use RIPE Atlas' VPs, we approximate a full 662 scan with probes to 12 of the DNS root server systems (G-Root was unavailable in 2021q3). 663 Although far fewer than 5M networks, these targets provide a very sparse sample of usually 664 independent destinations since each is independently operated. Thus we have complementary 665 datasets with sparse VPs and dense probing, and many VPs but sparse probing. In other 666 words, to get many VP locations we relax our conceptual definition by decreasing our target 667 list.

668 Figure 5a shows the CDF of the number of islands detected per RIPE Atlas VP during 669 2021q3. During this period, 55% of VPs observed one or no islands (the solid line). We 670 compare to Trinocular with only events longer than 660s (the dashed line). We see that 60% 671 of VPs have no islands; 19%, one; with 21% seeing more. The annualized rate of the stable 672 VPs that see 2 or fewer islands is 1.75 islands per year (a lower bound, since we exclude less 673 stable VPs), compared to 1.28 for Trinocular (Table 4b). We see islands are more common 674 in Atlas, perhaps because it includes many VPs in homes.

675 We conclude that islands *do* happen, but rarely, and occur at irregular times. This 676 finding is consistent with importance of the Internet at the locations where we run VPs.

677 **5.6 How Long Do Islands Last?**

678 Islands causes range from brief connectivity loss to long-term policy differences, so we next
 679 evaluate island duration.

680 We compare the distributions of island durations observed from RIPE Atlas (the left line)
 681 and Trinocular (right) in [Figure 5b](#). Since Atlas' frequent polling means it detects islands
 682 lasting seconds, while Trinocular sees only islands of 660 s or longer, we split out Atlas events
 683 lasting at least 660 s (middle line). All measurements follow a similar S-shaped curve, but
 684 for Trinocular, the curve is truncated at 660 s. With only 6 VPs, Trinocular sees far fewer
 685 events (23 in 3 years compared to 235k in a yearly quarter with Atlas), so the Trinocular
 686 data is quantized. In both cases, about 70% of islands are between 1000 and 6000 s. This
 687 graph shows that Trinocular's curve is similar in shape to Atlas-660 s, but about 2× longer.
 688 All Trinocular observers are in datacenters, while Atlas devices are often at homes, so this
 689 difference may indicate that datacenter islands are rarer, but harder to resolve.

690 **5.7 What Sizes Are Islands?**691 **5.7.1 Island Size via Traceroute**

692 First we evaluate island sizes, comparing traceroutes before and during an island. We use
 693 traceroutes from RIPE Atlas VPs sent to 12 root DNS servers for 2021q3 [\[70\]](#). [Figure 5c](#)
 694 shows the distribution of number of traceroute hops reaching target (green), and *not* reaching
 695 their target (purple), for VPs in islands ([§5.5](#)).

696 Most islands are small, with 70% at 0 or 1 hop. We believe huge islands (10 or more
 697 hops) are likely false positives.

698 **5.7.2 Country-sized Islands**

699 We have some evidence of country-sized islands: In 2017q3, on 8 occasions it appears that
 700 most or all of China stopped responding to external pings (visualized in [Figure 10](#) in [§C.1](#)).
 701 We found no problem reports on network operator mailing lists, so we believe these outages
 702 were ICMP-specific and likely did not affect web traffic. Since there were no public reports,
 703 we assume the millions of computers inside China continued to operate, suggesting that
 704 China was briefly a country-wide *ICMP-island*. Such large examples have not re-occurred.

705 **6 Applying These Tools**706 **6.1 Can the Internet Core Partition?**

707 In [§6.2](#) we discussed secession and expulsion qualitatively. Here we ask: Does any country or
 708 group have enough addresses to secede and claim to be “the Internet core” with a majority
 709 of addresses? Alternatively, if a country were to exert control over their allocated addresses,
 710 would they become a country-sized island or peninsula? We next use our reachability
 711 definition of more than 50% to quantify control of the IP address space.

712 To evaluate the power of countries and Regional Internet Registries (RIRs) over the
 713 Internet core, Table 6 reports the number of active IPv4 addresses as determined by Internet
 714 censuses [\[51\]](#) for RIRs and selected countries. Since estimating active IPv6 addresses is an
 715 open problem, we provide allocated addresses for both v4 and v6 [\[53, 54\]](#). (IPv4 has been
 716 fully allocated since 2011 [\[55\]](#)).

717 Table 6 shows that *no individual RIR or country can secede and take the Internet core*,
 718 because none controls the majority of IPv4 addresses. ARIN has the largest share with

719 1673M allocated (45.2%). Of countries, U.S. has the largest share of allocated IPv4 (1617M, 720 43.7%). Active addresses are more evenly distributed with APNIC (223M, 33%) and the 721 U.S. (40M, 21%) the largest RIR and country.

722 *IPv6 is also an international collaboration*, since no RIR or country surpasses a 50% 723 allocation for control. RIPE (an RIR) is close with 46.7%, and China and the U.S. have 724 large allocations; with most v6 unallocated, this balance may change.

725 IPv4 reflects a first-mover bias, where early adopters acquired many addresses, but this 726 factor is smaller in IPv6. Our definition's use of active addresses also reduces this bias, 727 since numbers of *active* IPv4 addresses is similar to allocated IPv6 addresses (legacy IPv4 728 addresses are less used).

729 6.2 Other Applications of the Definition

730 We next examine how a clear definition of the Internet core can inform policy tussles [21]. 731 Our hope is that our conceptual definition can make sometimes amorphous concepts like 732 “Internet fragmentation” more concrete, and an operational definition can quantify impacts 733 and identify thresholds.

734 **Secession and Sovereignty:** The U.S. [84], China [4, 5], and Russia [22] have all 735 proposed unplugging from the Internet. Egypt did in 2011 [25], and several countries have 736 during exams [45, 30, 52, 37]. When the Internet partitions, which part is still “the Internet 737 core”? Departure of an ISP or small country do not change the Internet core much, but what 738 if a large country, or group of countries, leave together? Our definition (§2.1) resolves this 739 question, since requiring a majority defines an Internet core that can end (§6.1) if multiple 740 partitions leave none with a majority.

741 **Sanction:** An opposite of secession is expulsion. Economic sanctions are one method of 742 asserting international influence, and events such as the 2022 war in Ukraine prompted several 743 large ISPs to discontinue service to Russia [80]. De-peering does not affect reachability for 744 ISPs that purchase transit, but Tier-1 ISPs that de-peer create peninsulas for their users. As 745 described below in §6.1, *no single country can eject another by de-peering with it*. However, 746 a coalition of multiple countries could de-peer and eject a country from the Internet core if 747 they, together, control more than half of the address space.

748 **Repurposing Addresses:** Given full allocation of IPv4, multiple parties proposed 749 re-purposing currently allocated or reserved IPv4 space, such 0/8 (“this” network), 127/8 750 (loopback), and 240/4 (reserved) [43]. New use of these long-reserved addresses is challenged 751 by assumptions in widely-deployed, difficult to change, existing software and hardware. Our 752 definition demonstrates that an RFC re-assigning this space for public traffic cannot make it 753 a truly effective part of the Internet core until implementations used by a majority of active 754 addresses can route to it.

755 **IPv4 Squat Space:** IP squatting is when an organization requiring private address 756 space beyond RFC1918 takes over allocated but currently unrouted IPv4 space [8]. Several 757 IPv4 /8s allocated to the U.S. DoD have been used this way [82] (they were only publicly 758 routed in 2021 [95]). By our definition, such space is not part of the Internet core without 759 public routes, and if more than half of the Internet is squatting on it, reclamation may be 760 challenging.

761 **The IPv4/v6 Transition:** We have defined two Internet cores: IPv4 and IPv6. Our 762 definition can determine when one supersedes the other. After more than half of all IPv4 763 hosts are dual-homed, IPv6 will supersede IPv4 when a majority of hosts on IPv6 can no 764 longer reach IPv4. Current limits on IPv6 measurement mean evaluation here is future 765 work, and show the strength and limits of our definition: since IPv6 is already economically

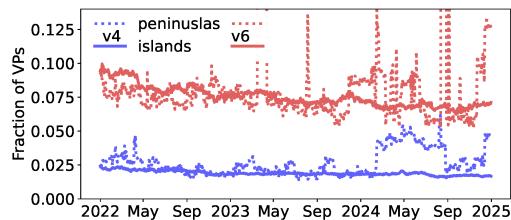


Figure 7 Fraction of VPs observing islands and peninsulas for IPv4 and IPv6, 2022–2025.

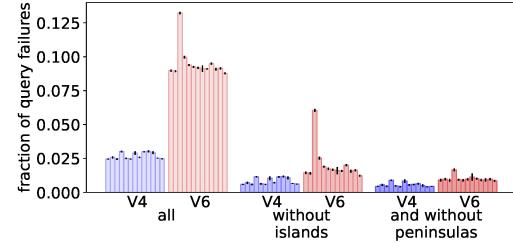


Figure 8 Atlas queries from all available VPs to 13 Root Servers for IPv4 and IPv6 on 2022-07-23.

important, a definition seems unnecessary. But providing a sharp threshold that makes the maturity of IPv6 definitive may help motivate late-movers.

Outage Detection: Prior outage detection systems have struggled with conflicting observations [90, 75, 91, 81, 49]. We instead recognize such cases as peninsulas in a normal Internet, not measurement error. (We expand in §6.4.)

6.3 Improving DNSmon Sensitivity

DNSmon [1] monitors the Root Server System [85], with each RIPE Atlas VP measuring its anycast-determined neighbor [83]. For years, DNSmon has often reported IPv6 loss rates of 4–10%. Since the DNS root is well provisioned and anycast, we expect minimal or no loss.

RIPE Atlas operators are aware of problems with some Atlas VPs. Some VPs support IPv6 on their LAN, but not to the global IPv6 Internet—such VPs are IPv6 islands. Atlas periodically tags and culls these VPs from DNSmon. However, our study of DNSmon for islands and peninsulas improves their results. Using concepts pioneered here (§2 and §3), we give full analysis in a workshop paper [87]; Here we add new data showing these results persist for 3 years (Figure 7).

Groups of bars in Figure 8 show query loss for each of the 13 root service identifiers, as observed from all available Atlas VPs (10,082 IPv4, and 5,173 IPv6) on 2022-07-23. (We are similar to DNSmon, but it uses only about 100 well-connected “anchors”, so our analysis is wider.) The first two groups show loss rates for IPv4 (light blue, left most) and IPv6 (light red), showing IPv4 losses around 2%, and IPv6 from 9 to 13%.

We apply Chiloe to these VPs, detecting as islands those VPs that cannot see *any* of the 13 root identifiers over 24 hours. (This definition is stricter than regular Chiloe because these VPs attempt only 13 targets, and we apply it over a full day to consider only long-term trends.) The middle two groups of bars show IPv4 and IPv6 loss rates after removing 188 v4 and 388 v6 VPs that are islands. Without islands, v4 loss drops to 0.005 from 0.01, and v6 to 0.01 from 0.06. These rates represent a more meaningful estimate of DNS reliability. Users of VPs that are IPv6 islands will not expect global IPv6, and such VPs should not be used for IPv6 in DNSmon.

The third bar in each red cluster of IPv6 is an outlier: that root identifier shows 13% IPv6 loss with all VPs, and 6% loss after islands are removed. This result is explained by persistent routing disputes between Cogent (the operator of C-Root) and Hurricane Electric [67]. Omitting islands (the middle bars) makes this difference much clearer.

Applying Taitao to detect peninsulas, we find 14 to 57 v4 peninsulas and 266 (Cogent) and 19 to 49 (others) v6 peninsulas. Peninsulas suggest persistent routing problems meriting attention from ISPs and root operators. The darker, right two groups show loss remaining (after removal of islands and peninsulas), representing *underlying events worth root operator*

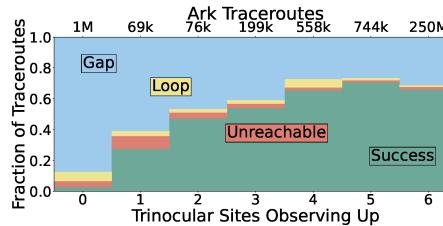


Figure 9 Ark traceroutes sent to targets under partial outages (2017-10-10 to -31). Dataset A30.

attention. These bars show all letters see similar events rates, *after* we remove persistent problems.

This example shows how *understanding partial reachability can improve the sensitivity of existing measurement systems*. Removing islands makes it easy to identify persistent routing problems. Removing peninsulas makes transient changes (perhaps from failure, DDoS, routing) more visible. Each layer of these problems can be interesting, but considering each separately, the interesting “signal” of routing changes (appearing in the right two groups in Figure 8), is hidden under the 5× or 9.7× times larger peninsulas and islands (the left two groups). Improved sensitivity also *shows a need to improve IPv6 provisioning*, since IPv6 loss is statistically higher than IPv4 loss (compare the right blue and red groups), even accounting for known problems. After sharing the results with root operators and RIPE Atlas, two operators adopted them in regular operation.

6.4 Outages Given Partial Reachability

We next re-evaluate reports from existing outage detection systems, considering how to resolve conflicting information in light of our new algorithms. We compare findings to external information in traceroutes from CAIDA Ark.

Figure 9 compares Trinocular with 21 days of Ark topology data, from 2017-10-10 to -31 from all 3 probing teams. For each Trinocular outage we classify the Ark result as success or three types of failure: unreachable, loop, or gap.

Trinocular’s 6-site-up case suggests a working network, and we consider this case as typical. However, we see that about 25% of Ark traceroutes are “gap”, where several hops fail to reply. We also see about 2% of traceroutes are unreachable (after we discard traceroutes to never reachable addresses). Ark probes a random address in each block; many addresses are non-responsive, explaining these.

With 1 to 11 sites up, Trinocular is reporting disagreement. We see that the number of Ark success cases (the green, lower portion of each bar) falls roughly linearly with the number of successful observers. This consistency suggests that Trinocular and Ark are seeing similar behavior, and that there is partial reachability—these events with only partial Trinocular positive results are peninsulas.

Since 5 sites give the same results as all 6, single-VP failures likely represent problems local to that VP. This data suggests that all-but-one voting will track true outages.

With only partial reachability, with 1 to 4 VPs (of 6), we see likely peninsulas. These cases confirm that partial connectivity is common: while there are 1M traceroutes sent to outages where no VP can see the target (the number of events is shown on the 0 bar), there are 1.6M traceroutes sent to partial outages (bars 1 to 5), and 850k traceroutes sent to definite peninsulas (bars 1 to 4). This result is consistent with the convergence we see in Figure 2.

839 **7 Related Work**

840 Prior definitions of the Internet exist at the IP-layer [18, 73, 41, 39] of their time, or the
 841 AS-level [44, 63]. We consider the IP-layer, and seek to address today’s challenges (see §2).

842 Cannon explored legal definitions of the Internet [16], recognizing limitations of early
 843 definitions and need to be application-independent. Like us, he considers connectivity and
 844 addressing important, but he questions if a firm legal definition is possible. While we do not
 845 comment legalities, we suggest our technical definition may address his questions.

846 Several systems mitigate partial outages. RON provides alternate-path routing around
 847 failures for a mesh of sites [2]. Hubble monitors in real-time reachability problems when
 848 working physical paths exist [57]. LIFEGUARD, remediates route failures by rerouting traffic
 849 using BGP to select a working path [58]. While addressing the problem of partial outages,
 850 these systems do not quantify their duration or scope.

851 Prior work studied partial reachability, showing it is a common transient occurrence during
 852 routing convergence [12]. They reproduced partial connectivity with controlled experiments;
 853 we study it from Internet-wide VPs.

854 Internet scanners have examined bias by location [51], more recently looking for policy-
 855 based filtering [99]. We measure policies with our country specific algorithm, and we extend
 856 those ideas to defining the Internet core.

857 Active outage detection systems have encountered partial outages. Thunderping’s “hosed”
 858 state recognizes mixed replies, but its study is future work [90]. Trinocular discards partial
 859 outages by reporting the target block “up” if any VP can reach it [75]. Disco identifies partial
 860 connectivity as future work [91]. None of these systems consistently report partial outages in
 861 the Internet core, nor study their extent.

862 We use the idea of majority to define the Internet core in the face of secession. That idea
 863 is fundamental in many algorithms for distributed consensus [61, 60, 68], for example, with
 864 applications to certificate authorities [11].

865 Recent work considered policies about Internet fragmentation [33, 34], but do not define
 866 it—a need we hope to meet.

867 **8 Conclusions**

868 Our new definition of the Internet core leads to new algorithms: Taitao, to find peninsulas
 869 of partial connectivity, and Chiloe, to find islands. We validate these algorithms and show
 870 partial reachability is as common as simple outages. They have important applications about
 871 Internet sovereignty and to improve outage and DNSmon measurement systems.

872 **References**

- 873 1 Christopher Amin, Massimo Cándela, Daniel Karrenberg, Robert Kisteleki, and Andreas
 874 Strikos. Visualization and monitoring for the identification and analysis of DNS issues.
 875 In *Proceedings of the International Conference on the Internet Monitoring and Protection*,
 876 Brussels, Belgium, June 2015.
- 877 2 David G. Andersen, Hari Balakrishnan, M. Frans Kaashoek, and Robert Morris. Resilient
 878 overlay networks. In *Proceedings of the Symposium on Operating Systems Principles*, pages
 879 131–145, Chateau Lake Louise, Alberta, Canada, October 2001. ACM.
- 880 3 Nate Anderson. Peering problems: digging into the Comcast/Level 3 grudgematch.
 881 *Ars Technica*, Dec. 9 2010. URL: <https://arstechnica.com/tech-policy/2010/12/comcastlevel3/>.

883 4 Anonymous. The collateral damage of Internet censorship by DNS injection. *ACM Computer*
884 *Communication Review*, 42(3):21–27, July 2012. [doi:10.1145/2317307.2317311](https://doi.org/10.1145/2317307.2317311).

885 5 Anonymous. Towards a comprehensive picture of the Great Firewall’s DNS censorship. In
886 *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet*,
887 San Diego, CA, USA, August 2014. USENIX.

888 6 ANT Project. Ant internet islands and peninsula datasets. https://ant.isi.edu/datasets/ipv4_partial/, January 2017. URL: https://ant.isi.edu/datasets/ipv4_partial/.

890 7 ANT Project. ANT IPv4 island and peninsula data. [https://ant.isi.edu/datasets/ipv4_](https://ant.isi.edu/datasets/ipv4_partial/)
891 [partial/](https://ant.isi.edu/datasets/ipv4_partial/), November 2022.

892 8 Cathy Aronson. To squat or not to squat? blog [https://teamarin.net/2015/11/23/](https://teamarin.net/2015/11/23/to-squat-or-not-to-squat/)
893 [to-squat-or-not-to-squat/](https://teamarin.net/2015/11/23/to-squat-or-not-to-squat/), November 2015.

894 9 Guillermo Baltra, Tarang Saluja, Yuri Pradkin, and John Heidemann. Understanding partial
895 reachability in the internet core (extended). Technical Report arXiv:2601.12196, arXiv, January
896 2026. The technical report includes additional appendices. [doi:doi:10.48550/arXiv.2601.](https://doi.org/10.48550/arXiv.2601.12196)
897 [12196](https://doi.org/10.48550/arXiv.2601.12196).

898 10 Genevieve Bartlett, John Heidemann, and Christos Papadopoulos. Understanding passive and
899 active service discovery. In *Proceedings of the ACM Internet Measurement Conference*, pages
900 57–70, San Diego, California, USA, October 2007. ACM. [doi:10.1145/1298306.1298314](https://doi.org/10.1145/1298306.1298314).

901 11 Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal.
902 Bamboozing certificate authorities with BGP. In *27th USENIX Security Symposium*, pages
903 833–849, Baltimore, Maryland, USA, 2018. USENIX.

904 12 Randy Bush, Olaf Maennel, Matthew Roughan, and Steve Uhlig. Internet optometry: assessing
905 the broken glasses in internet reachability. In *Proceedings of the 9th ACM SIGCOMM conference*
906 *on Internet measurement*, pages 242–253, Chicago, Illinois, USA, November 2009. ACM. URL:
907 <http://www.maennel.net/2009/imc099-bush.pdf>.

908 13 CAIDA. Archipelago (Ark) measurement infrastructure. website <https://www.caida.org/projects/ark/>, 2007.

909 14 CAIDA. The CAIDA UCSD IPv4 routed /24 topology dataset - 2017-10-10 to -31. https://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml, 2017.

910 15 CAIDA. The CAIDA UCSD IPv4 routed /24 topology dataset - 2020-09-01 to -31. https://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml, 2020.

911 16 Robert Cannon. Will the real Internet please stand up: An attorney’s quest to define the
912 internet. In *Proceedings of the TPRC, the Research Conference on Communication, Information*
913 *and Internet Policy*. TPRC, March 2002. Also in: *Rethinking Rights and Regulations*. [doi:10.7551/mitpress/5932.003.0007](https://doi.org/10.7551/mitpress/5932.003.0007).

914 17 Ben Cartwright-Cox. Cogent-tata peering dispute? Nanog mailing list, May 17 2024. URL:
915 <https://mailman.nanog.org/pipermail/nanog/2024-May/225651.html>.

916 18 Vint Cerf and Robert Kahn. A protocol for packet network interconnection. *IEEE Transactions*
917 *on Communications*, COM-22(5):637–648, May 1974.

918 19 S. Cheshire and M. Krochmal. NAT port mapping protocol (NAT-PMP). RFC 6886, Internet
919 Request For Comments, April 2013. [doi:10.17487/RFC6886](https://doi.org/10.17487/RFC6886).

920 20 David D. Clark. The design philosophy of the DARPA Internet protocols. In *Proceedings of*
921 *the 1988 Symposium on Communications Architectures and Protocols*, pages 106–114. ACM,
922 August 1988.

923 21 David D. Clark, John Wroclawski, Karen Sollins, and Robert Braden. Tussle in cyberspace:
924 Defining tomorrow’s internet. In *Proceedings of the ACM SIGCOMM Conference*, pages
925 347–356, Pittsburgh, PA, USA, August 2002. ACM.

926 22 CNBC. Russia just brought in a law to try to disconnect its
927 Internet from the rest of the world. [https://www.cnbc.com/2019/11/01/](https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html)
928 [russia-controversial-sovereign-internet-law-goes-into-force.html](https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html), 11 2019.

929 930 931 932

933 23 N. Coca. China's xinjiang surveillance is the dystopian future nobody
 934 wants. *Engadget*, Feb. 22 2018. URL: <https://www.engadget.com/2018-02-22-china-xinjiang-surveillance-tech-spread.html>.

935 24 Cogent. Looking glass. <https://cogentco.com/en/looking-glass>, 05 2021.

936 25 James Cowie. Egypt leaves the Internet. Renesys Blog <http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml>, January 2011.

937 26 RBC daily. Russia, tested the Runet when disconnected from the global network. website https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739, July 2021.

938 27 Alberto Dainotti, Karyn Benson, Alistair King, kc claffy, Eduard Glatz, Xenofontas
 939 Dimitropoulos, Philipp Richter, Alessandro Finamore, and Alex C. Snoeren. Lost in space:
 940 Improving inference of IPv4 address space utilization. *IEEE Journal of Selected Areas in
 941 Communication*, 34(6):1862–1876, April 2016. doi:10.1109/JSAC.2016.2559218.

942 28 Alberto Dainotti, kc claffy, Alistair King, Vasco Asturiano, Karyn Benson, Marina Fomenkov,
 943 Brad Huffaker, Young Hyun, Ken Keys, Ryan Koga, Alex Ma, Chiara Orsini, and Josh
 944 Polterock. IODA: Internet outage detection & analysis. Talk at CAIDA Active Internet
 945 Measurement Workshop (AIMS), March 2017. URL: http://www.caida.org/publications/presentations/2017/ioda_aims/ioda_aims.pdf.

946 29 Alberto Dainotti, Claudio Squarcella, Emile Aben, Marco Chiesa, Kimberly C. Claffy, Michele
 947 Russo, and Antonio Pescapé. Analysis of country-wide Internet outages caused by censorship.
 948 In *Proceedings of the ACM Internet Measurement Conference*, pages 1–18, Berlin, Germany,
 949 November 2011. ACM. doi:10.1145/2068816.2068818.

950 30 Dhaka Tribune Desk. Internet services to be suspended across the country. *Dhaka Tribune*,
 951 Feb. 11 2018. URL: <http://www.dhakatribune.com/regulation/2018/02/11/internet-services-suspended-throughout-country>.

952 31 Amogh Dhamdhare, David D. Clark, Alexander Gamero-Garrido, Matthew Luckie, Ricky K. P.
 953 Mok, Gautam Akiwate, Kabir Gogia, Vaibhav Bajpai, Alex C. Snoeren, and kc claffy. Inferring
 954 persistent interdomain congestion. In *Proceedings of the ACM SIGCOMM Conference*, pages
 955 1–15, Budapest, Hungary, August 2018. ACM. doi:10.1145/3230543.3230549.

956 32 DINRG. Decentralized Internet Infrastructure Research Group. <https://irtf.org/dinrg>, 05
 957 2021.

958 33 William J. Drake, Vinton G. Cerf, and Wolfgang Kleinwächter. Internet fragmentation: An
 959 overview. Technical report, World Economic Forum, January 2016. URL: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

960 34 William J. Drake (moderator). Internet fragmentation, reconsidered. CITI Seminar on Global
 961 Digital Governance at IETF 115, October 2022. URL: <https://www8.gsb.columbia.edu/citi/GlobalDigitalGovernance>.

962 35 Peter K. Dunn. Scientific research methods. <https://bookdown.org/pkaldunn/Book/>, 05
 963 2021.

964 36 Zakir Durumeric, Michael Bailey, and J Alex Halderman. An internet-wide view of internet-
 965 wide scanning. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 65–78,
 966 San Diego, California, USA, August 2014. USENIX.

967 37 Economist Editors. Why some countries are turning off the internet on exam
 968 days. *The Economist*, July 5 2018. (Appeared in the Middle East and Africa
 969 print edition). URL: <https://www.economist.com/middle-east-and-africa/2018/07/05/why-some-countries-are-turning-off-the-internet-on-exam-days>.

970 38 Hurricane Electric. Looking glass. <http://lg.he.net/>, May 2021.

971 39 Engadget. China, Huawei propose internet protocol with a built-in killswitch. <https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html>, 2020.

972 40 Xun Fan and John Heidemann. Selecting representative IP addresses for Internet topology
 973 studies. In *Proceedings of the ACM Internet Measurement Conference*, pages 411–423,
 974 Melbourne, Australia, November 2010. ACM. doi:10.1145/1879141.1879195.

984 41 Federal Networking Council (FNC). Definition of “Internet”. https://www.nitrd.gov/historical/fnc/internet_res.pdf, 1995.

985 42 HE forums. Cloudflare blocked on free tunnels now? <https://forums.he.net/index.php?topic=3805.0>, 12 2017.

986 43 V. Fuller, E. Lear, and D. Meyer. Reclassifying 240/4 as usable unicast address space. Work in progress (Internet draft draft-fuller-240space-02.txt), March 2008. URL: <https://datatracker.ietf.org/doc/html/draft-fuller-240space-02>.

987 44 Lixin Gao. On inferring autonomous system relationships in the Internet. *ACM/IEEE Transactions on Networking*, 9(6):733–745, December 2001. doi:10.1109/90.974527.

988 45 Samuel Gibbs. Iraq shuts down the Internet to stop pupils cheating in exams. *The Guardian*, 18 May 1996. URL: <https://www.theguardian.com/technology/2016/may/18/iraq-shuts-down-internet-to-stop-pupils-cheating-in-exams>.

989 46 GovTrack.us. Unplug the Internet Kill Switch Act would eliminate a 1942 law that could let the president shut down the internet. <https://govtrackinsider.com/unplug-the-internet-kill-switch-act-would-eliminate-a-1942-law-that-could-let-the-president-shut-78326> November 2020.

990 47 Albert Greenberg, James R. Hamilton, Navendu Jain, Srikanth Kandula, Changhoon Kim, Parantap Lahiri, David A. Maltz, and Parveen Pat. VL2: A scalable and flexible data center network. In *Proceedings of the ACM SIGCOMM Conference*, pages 51–62, Barcelona, Spain, August 2009. ACM.

991 48 James Griffiths. Democratic Republic of Congo internet shutdown shows how chinese censorship tactics are spreading. *CNN*, Jan. 2 2019. URL: <https://edition.cnn.com/2019/01/02/africa/congo-internet-shutdown-china-intl/index.html>.

992 49 Andreas Guillot, Romain Fontugne, Philipp Winter, Pascal Merindol, Alistair King, Alberto Dainotti, and Cristel Pelsser. Chocolatine: Outage detection for internet background radiation. In *Proceedings of the IFIP International Workshop on Traffic Monitoring and Analysis*, Paris, France, June 2019. IFIP.

993 50 Hang Guo and John Heidemann. Detecting ICMP rate limiting in the Internet. In *Proceedings of the Passive and Active Measurement Workshop*, page to appear, Berlin, Germany, March 2018. Springer.

994 51 John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett, and Joseph Bannister. Census and survey of the visible Internet. In *Proceedings of the ACM Internet Measurement Conference*, pages 169–182, Vouliagmeni, Greece, October 2008. ACM. doi:10.1145/1452520.1452542.

995 52 Jon Henley. Algeria blocks internet to prevent students cheating during exams. *The Guardian*, 22 June 2018. URL: <https://www.theguardian.com/world/2018/jun/21/algeria-shuts-internet-prevent-cheating-school-exams>.

996 53 IANA. IPv4 address space registry. <https://www.nro.net/about/rirs/statistics/>, 05 2021.

997 54 IANA. IPv6 RIR allocation data. <https://www.iana.org/numbers/allocations/>, 01 2021.

998 55 ICANN. Available pool of unallocated IPv4 internet addresses now completely emptied. Announcement, ICANN, February 2011. URL: <https://itp.cdn.icann.org/en/files/announcements/release-03feb11-en.pdf>.

999 56 Internet Architecture Board. IAB technical comment on the unique DNS root. RFC 2826, Internet Request For Comments, May 2000. URL: <https://www.rfc-editor.org/rfc/rfc2826>.

1000 57 Ethan Katz-Bassett, Harsha V Madhyastha, John P John, Arvind Krishnamurthy, David Wetherall, and Thomas E Anderson. Studying black holes in the internet with hubble. In *Proceedings of the USENIX Conference on Networked Systems Design and Implementation*, pages 247–262, San Francisco, CA, 2008. ACM.

1001 58 Ethan Katz-Bassett, Colin Scott, David R. Choffnes, Ítalo Cunha, Vytautas Valancius, Nick Feamster, Harsha V. Madhyastha, Tom Anderson, and Arvind Krishnamurthy. LIFEGUARD:

1036 Practical repair of persistent route failures. In *Proceedings of the ACM SIGCOMM Conference*,
 1037 pages 395–406, Helsinki, Finland, August 2012. ACM. [doi:10.1145/2377677.2377756](https://doi.org/10.1145/2377677.2377756).

1038 59 Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian.
 1039 Internet inter-domain traffic. In *Proceedings of the ACM SIGCOMM Conference*, pages 75–86,
 1040 New Delhi, India, August 2010. ACM. [doi:10.1145/1851182.1851194](https://doi.org/10.1145/1851182.1851194).

1041 60 Leslie Lamport. The part-time parliament. *ACM Transactions on Computer Systems*, 16(2):133–
 1042 169, May 1998. [doi:https://doi.org/10.1145/279227.279229](https://doi.org/10.1145/279227.279229).

1043 61 Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM
 1044 Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

1045 62 Mike Leber. Re: Ipv6 internet broken, cogent/telia/hurricane not peering. NANOG mailing list,
 1046 October 2009. URL: <https://mailman.nanog.org/pipermail/nanog/2009-October/014017.html>.

1047 63 Matthew Luckie, Bradley Huffaker, Dhamdhere, Vasileios Giotsas, and kc claffy. AS
 1048 relationships, customer cones, and validation. In *Proceedings of the ACM Internet Measurement
 1049 Conference*, pages 243–256, Barcelona, Spain, October 2013. ACM.

1050 64 Ratul Mahajan, David Wetherall, and Tom Anderson. Understanding BGP misconfiguration.
 1051 In *Proceedings of the ACM SIGCOMM Conference*, pages 3–16, Pittsburgh, Pennsylvania,
 1052 USA, August 2002. ACM. [doi:10.1145/633025.633027](https://doi.org/10.1145/633025.633027).

1053 65 D. Meyer. University of Oregon Routeviews. <http://www.routeviews.org>, 2018.

1054 66 Brent A. Miller, Toby Nixon, Charlie Tai, and Mark D. Wood. Home networking with
 1055 universal plug and play. *IEEE Communications Magazine*, 39(12):104–109, December 2001.
 1056 [doi:10.1109/35.968819](https://doi.org/10.1109/35.968819).

1057 67 Rich Miller. Peering disputes migrate to IPv6. website <https://www.datacenterknowledge.com/archives/2009/10/22/peering-disputes-migrate-to-ipv6>, Oct. 22 2009.

1058 68 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Released publically
 1059 <http://bitcoin.org/bitcoin.pdf>, March 2009.

1060 69 RIPE NCC. RIPE atlas IP echo measurements in IPv4. [https://atlas.ripe.net/measurements/\[1001,1004,1005,1006,1008,1009,1010,1011,1012,1013,1014,1015,1016\]/](https://atlas.ripe.net/measurements/[1001,1004,1005,1006,1008,1009,1010,1011,1012,1013,1014,1015,1016]/), 2021q3.

1061 70 RIPE NCC. RIPE atlas IP traceroute measurements in IPv4. [https://atlas.ripe.net/measurements/\[5001,5004,5005,5006,5008,5009,5010,5011,5012,5013,5014,5015,5016\]/](https://atlas.ripe.net/measurements/[5001,5004,5005,5006,5008,5009,5010,5011,5012,5013,5014,5015,5016]/), 2021q3.

1062 71 BBC News. Russia internet: Law introducing new controls comes into force. website <https://www.bbc.com/news/world-europe-50259597>, March 2019.

1063 72 Ramakrishna Padmanabhan, Amogh Dhamdhere, Emile Aben, kc claffy, and Neil Spring.
 1064 Reasons dynamic addresses change. In *Proceedings of the ACM Internet Measurement
 1065 Conference*, pages 183–198, Santa Monica, CA, USA, November 2016. ACM. [doi:10.1145/2987443.2987461](https://doi.org/10.1145/2987443.2987461).

1066 73 Jonathan B. Postel. Internetwork protocol approaches. *IEEE Transactions on Computers*,
 1067 28(4):604–611, April 1980. [doi:10.1109/TCOM.1980.1094705](https://doi.org/10.1109/TCOM.1980.1094705).

1068 74 Matthew Prince. Cloudflare outage on November 18, 2025. Cloudflare blog <https://blog.cloudflare.com/18-november-2025-outage/>, November 2025.

1069 75 Lin Quan, John Heidemann, and Yuri Pradkin. Trinocular: Understanding Internet reliability
 1070 through adaptive probing. In *Proceedings of the ACM SIGCOMM Conference*, pages 255–266,
 1071 Hong Kong, China, August 2013. ACM. [doi:10.1145/2486001.2486017](https://doi.org/10.1145/2486001.2486017).

1072 76 Dan Rayburn. Google blocking IPv6 adoption with Cogent, impacting transit customers.
 1073 <https://seekingalpha.com/article/3948876-google-blocking-ipv6-adoption-cogent-impacting-transit-customers>, 03
 1074 2016.

1075 77 Dan Rayburn. Google blocking IPv6 adoption with Cogent, impacting transit customers.
 1076 web page <https://seekingalpha.com/article/3948876-google-blocking-ipv6-adoption-cogent-impacting-transit-customers>,

1088 March 2016. URL: <https://seekingalpha.com/article/3948876-google-blocking-ipv6-adoption-cogent-impacting-transit-customers>.

1089 78 Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. Address allocation for private internets. RFC 1918, Internet Request For Comments, February 1996.

1090 79 Reuters. Russia disconnected from internet in tests as it bolsters security. website <https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/>, July 2021. URL: <https://www.reuters.com/technology/russia-disconnected-global-internet-tests-rbc-daily-2021-07-22/>.

1091 80 Reuters. website <https://www.reuters.com/technology/us-firm-cogent-cutting-internet-service-russia-2022-03-04/>, July 2022. URL: <https://www.reuters.com/technology/us-firm-cogent-cutting-internet-service-russia-2022-03-04/>.

1092 81 Philipp Richter, Ramakrishna Padmanabhan, Neil Spring, Arthur Berger, and David Clark. Advancing the art of Internet edge outage detection. In *Proceedings of the ACM Internet Measurement Conference*, pages 350–363, Boston, Massachusetts, USA, October 2018. ACM. doi:10.1145/3278532.3278563.

1093 82 Philipp Richter, Florian Wohlfart, Narseo Vallina-Rodriguez, Mark Allman, Randy Bush, Anja Feldmann, Christian Kreibich, Nicholas Weaver, and Vern Paxson. A multi-perspective analysis of carrier-grade NAT deployment. In *Proceedings of the ACM Internet Measurement Conference*, Santa Monica, CA, USA, November 2016. ACM. doi:10.1145/2987443.2987474.

1094 83 RIPE NCC Staff. RIPE Atlas: A global Internet measurement network. *The Internet Protocol Journal*, 18(3):2–26, September 2015.

1095 84 Sen. John D. Rockefeller. Cybersecurity act of 2010. <https://www.congress.gov/bill/111th-congress/senate-bill/773>, 2009.

1096 85 Root Operators. <http://www.root-servers.org>, April 2016.

1097 86 J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. STUN—simple traversal of user datagram protocol (UDP) through network address translators (NATs). RFC 3489, Internet Request For Comments, December 2003.

1098 87 Tarang Saluja, John Heidemann, and Yuri Pradkin. Differences in monitoring the DNS root over IPv4 and IPv6. In *Proceedings of the National Symposium for NSF REU Research in Data Science, Systems, and Security*, page to appear, Portland, OR, USA, December 2022. IEEE.

1099 88 Tarang Saulja and Yuri Pradkin. RIPE Atlas islands and peninsulas. https://ant.isi.edu/ripe_atlas_islands/, September 2022.

1100 89 Brandon Schlinker, Hyojeong Kim, Timothy Cui, Ethan Katz-Bassett, Harsha V. Madhyastha, Italo Cunha, James Quinn, Saif Hasan, Petr Lapukhov, and Hongyi Zeng. Engineering egress with Edge Fabric: Steering oceans of content to the world. In *Proceedings of the ACM SIGCOMM Conference*, pages 418–431, Los Angeles, CA, USA, August 2017. ACM. doi:10.1145/3098822.3098853.

1101 90 Aaron Schulman and Neil Spring. Pingin’ in the rain. In *Proceedings of the ACM Internet Measurement Conference*, pages 19–25, Berlin, Germany, November 2011. ACM. doi:10.1145/2068816.2068819.

1102 91 Anant Shah, Romain Fontugne, Emile Aben, Cristel Pelsser, and Randy Bush. Disco: Fast, good, and cheap outage detection. In *Proceedings of the IEEE International Conference on Traffic Monitoring and Analysis*, pages 1–9, Dublin, Ireland, June 2017. Springer. doi:10.23919/TMA.2017.8002902.

1103 92 D. Smallberg. Who talks TCP? RFC 832, Internet Request For Comments, December 1982.

1104 93 Berhan Taye and Sage Cheng. Report: the state of internet shutdowns. blog <https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/>, 8 July 2019.

1105 94 ThinkBroadband. NTT/Cogent peering dispute increasing latency for some routes. <https://www.thinkbroadband.com/news/>

1140 9896-[ntt-cogent-peering-dispute-increasing-latency-for-some-routes](#), Feb. 16
 1141 2024.

1142 95 Craig Timberg and Paul Sonne. Minutes before Trump left office, millions of the Pentagon's
 1143 dormant IP addresses sprang to life. *The Washington Post*, Apr. 24 2021. URL: <https://www.washingtonpost.com/technology/2021/04/24/pentagon-internet-address-mystery/>.

1145 96 Paul F. Tsuchiya and Tony Eng. Extending the IP Internet through address reuse. *ACM Computer Communication Review*, 23(1):16–33, January 1993.

1147 97 USC/LANDER Project. Internet outage measurements. listed on web page <https://ant.isi.edu/datasets/outage/>, October 2014.

1149 98 USC/LANDER Project. Internet outage measurements. IMPACT ID [USC-LANDER/LANDER:internet_outage_adaptive_a30all-20171006](#) at https://ant.isi.edu/datasets/internet_outages/, October 2017.

1152 99 Gerry Wan, Liz Izhikevich, David Adrian, Katsunari Yoshioka, Ralph Holz, Christian Rossow,
 1153 and Zakir Durumeric. On the origin of scanning: The impact of location on internet-wide scans.
 1154 In *Proceedings of the ACM Internet Measurement Conference*, pages 662–679, Pittsburgh, PA,
 1155 USA, October 2020. ACM. [doi:10.1145/3419394.3424214](https://doi.org/10.1145/3419394.3424214).

1156 100 Feng Wang, Zhuoqing Morley Mao, Jia Wang, Lixin Gao, and Randy Bush. A measurement
 1157 study on the impact of routing events on end-to-end Internet path performance. In *Proceedings
 1158 of the ACM SIGCOMM Conference*, pages 375–386, Pisa, Italy, August 2006. ACM. [doi:10.1145/1159913.1159956](https://doi.org/10.1145/1159913.1159956).

1160 101 Samuel Woodhams and Simon Migliano. The global cost of internet shutdowns in 2020.
 1161 <https://www.top10vpn.com/cost-of-internet-shutdowns/>, 01 2021.

1162 102 Kok-Kiong Yap, Murtaza Motiwala, Jeremy Rahe, Steve Padgett, Matthew Holliman, Gary
 1163 Baldus, Marcus Hines, Tae-eun Kim, Ashok Narayanan, Ankur Jain, Victor Lin, Colin Rice,
 1164 Brian Rogan, Arjun Singh, Bert Tanaka, Manish Verma, Puneet Sood, Mukarram Tariq, Matt
 1165 Tierney, Dzevad Trumic, Vytautas Valancius, Calvin Ying, Mahesh Kallahalla, Bikash Koley,
 1166 and Amin Vahdat. Taking the edge off with Espresso: Scale, reliability and programmability
 1167 for global Internet peering. In *Proceedings of the ACM SIGCOMM Conference*, pages 432–445,
 1168 Los Angeles, CA, USA, August 2017. ACM. [doi:10.1145/3098822.3098854](https://doi.org/10.1145/3098822.3098854).

1169 103 Sebastian Zander, Lachlan L. H. Andrew, and Grenville Armitage. Capturing ghosts: Predicting
 1170 the used IPv4 space by inferring unobserved addresses. In *Proceedings of the ACM Internet
 1171 Measurement Conference*, pages 319–332, Vancouver, BC, Canada, November 2014. ACM.
 1172 [doi:10.1145/2663716.2663718](https://doi.org/10.1145/2663716.2663718).

A Discussion of Research Ethics

1174 Our work poses no ethical concerns as described in §1. We elaborate here.

1175 First, we collect no additional data, but instead reanalyze data from several existing
 1176 sources (see Appendix D.1 of [9]). Our work therefore poses no additional load on the
 1177 Internet, nor any new risk from data collection.

1178 Our analysis poses no risk to individuals because our subject is network topology and
 1179 connectivity. There is a slight risk to individuals in that we examine responsiveness of
 1180 individual IP addresses. With external information, IP addresses can sometimes be traced
 1181 to individuals, particularly when combined with external data sources like DHCP logs. We
 1182 avoid this risk in three ways. First, we do not have DHCP logs for any networks (and in
 1183 fact, most are unavailable outside of specific ISPs). Second, we commit, as research policy,
 1184 to not combine IP addresses with external data sources that might de-anonymize them to
 1185 individuals. Finally, except for analysis of specific cases as part of validation, all of our
 1186 analysis is done in bulk over the whole dataset.

1187 We do observe data about organizations such as ISPs, and about the geolocation of blocks
 1188 of IP addresses. Because we do not map IP addresses to individuals, this analysis poses no
 1189 individual privacy risk.

1190 Finally, we suggest that while our work poses minimal privacy risks to individuals, to
 1191 also provides substantial benefit to the community and to individuals. For reasons given in
 1192 the introduction it is important to improve network reliability and understand how networks
 1193 fail. Our work contributes to that goal.

1194 Our work was reviewed by the Institutional Review Board at our university and because
 1195 it poses no risk to individual privacy, it was identified as non-human subjects research (USC
 1196 IRB IIR00001648).

1197 B Proof of Majority Enforcing One or No Internet

1198 Our definition in §2.1 is complete, and Bitcoin provides an example of majority forcing
 1199 consensus. However, here we provide a proof and discuss scenarios that, at first glance, may
 1200 appear challenging.

1201 Our conceptual definition is “the strongly-connected component of more than 50% of
 1202 active, public IP addresses that can initiate communication with each other”, is chosen to
 1203 ensure there can be only one Internet in each address space (IPv4 and IPv6). We next prove
 1204 this definition yields one result, both with and without peninsulas.

1205 The reasoning for this choice in §2.1 is straightforward: if a connected component has
 1206 some fraction A , where $1 > A > 0.5$, than this component *must* be larger than any other
 1207 component B . One can prove this by contradiction: (i) assume some B' exists, such that
 1208 $B' > A$. (ii) Since $A > 0.5$, then (i) implies $B' > 0.5$. (iii) We then must conclude that
 1209 $A + B' > 1$, but by definition, we measure only the whole address space, so it is also required
 1210 that $A + B' \leq 1$. Therefore $B' < A$ and A forces a single clear component. Q.E.D.

1211 **Resolving competing “cores”:** This definition handles cases with multiple overlapping
 1212 but incompletely communicating groups. If members of those groups can reach half the
 1213 active addresses, they are part of the Internet even if some are on peninsulas relative to each
 1214 other. Consider a simplified version of Figure 1 with only three with three pluralities of
 1215 connectivity, A , B , and C , each representing one third of the addresses, where A and B are
 1216 strongly and directly connected, and A and C are strongly and directly connected, but B and
 1217 C cannot directly reach each other. (Recall that strong connections in graph theory means
 1218 bi-directional connectivity, but it does not require *direct* and allows connections through
 1219 multiple hops.) In this example, B and C can reach each other, but only through A , so
 1220 they are strongly connected but not directly connected. Our Internet core requires strong
 1221 connections, but if it required direct connections, it would become a clique (a fully connected
 1222 graph), forbidding peninsulas.

1223 In this example there are two, partially overlapping, large, components that are both
 1224 strongly and directly connected: $A \cup B$ and $A \cup C$. Here *all* ($A \cup B \cup C$) are part of the
 1225 Internet, because any address can directly reach more than half of the active addresses:
 1226 address $b \in B$ can reach $A \cup B$, $c \in C$ can reach $B \cup C$, and $a \in A$ can reach anyone. While
 1227 all addresses are in one Internet, B and C are on peninsulas. The example in Figure 1 is
 1228 similar to this thought experiment. In practice, we know that peninsulas occur in less than
 1229 1% of block-time (§5.1), so typically $A \geq 0.98$, with other components $B, C < 0.01$, quite
 1230 different from this theoretical case where $A = B = C = 0.33$, or an asymmetric case where
 1231 $A = 0.49$ and $B = C = 0.02$. However, the definition applies whenever $A \cup B \cup C > 0.5$.

1232 **Resolving disagreements with incomplete knowledge:** In the above discussion we

1233 apply our conceptual definition assuming an omniscience view of connectivity. All parties
 1234 must agree that A directly reaches both B and C , but B and C can reach each other only
 1235 indirectly through A . An omniscient observer must recognize they are all part of the same
 1236 core, in spite of the peninsula.

1237 In practice, no real-world system will have omniscient knowledge of connectivity. However,
 1238 this scenario works even with incomplete knowledge. Imagine observers only in B and C
 1239 both might assert they are “the” core, since both can observe direct, strong connectivity to
 1240 more than half of the active, public addresses.

1241 When faced with seemingly conflicting claims of what the core is, all parties must share
 1242 their observations with each other to make their case. In this case, B and C will recognize
 1243 they are both reporting A as part of their core, and that A overlaps—they must therefore
 1244 recognize the reachable core is $A \cup B \cup C$, even though they cannot directly reach each other.

1245 This seeming disagreement highlights the requirement that B and C recognize that the
 1246 A they each measure is the same A . This requirement is met by our definition of what a
 1247 public, global address space is—we assume some authority allocated addresses. In today’s
 1248 Internet, this authority is IANA. Note that IANA is not saying who is in or out of the
 1249 Internet, but only who is responsible for a given fraction of the address space.

1250 If all parties cannot agree on a shared address space, then our definition cannot be used.
 1251 For example, if one party asserts the entire 0/0 IPv4 address space is theirs to reallocate, then
 1252 one cannot use address to resolve disputes. Fortunately, address assignment has historically
 1253 been coordinated to avoid overlaps. (One exception is DISA’s 4 /8 prefixes. These were
 1254 clearly allocated to DISA, but lack of global routing prompted multiple organizations to
 1255 squat on them, using them as additional private address space. Fortunately this variance is
 1256 not a practical problem for several reasons: Since 2021 DISA has announced routes for these
 1257 blocks on the public Internet. Their actual allocation has never been disputed. And even if
 1258 they were disputed, this 4/256ths of the address space is not enough to change control of a
 1259 majority.)

1260 C Additional Results about Islands

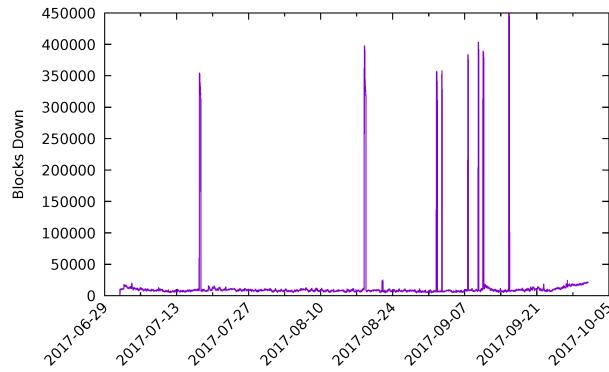
1261 We define islands and give examples in §2.3.2. Here we supplement those results with
 1262 examples of country-sized islands (§5.7.2). We also show the raw data we use to justify our
 1263 choice of 50% unreachability to define islands in Trinocular (§C.2).

1264 C.1 Visualizing Potential 2017q3 Islands

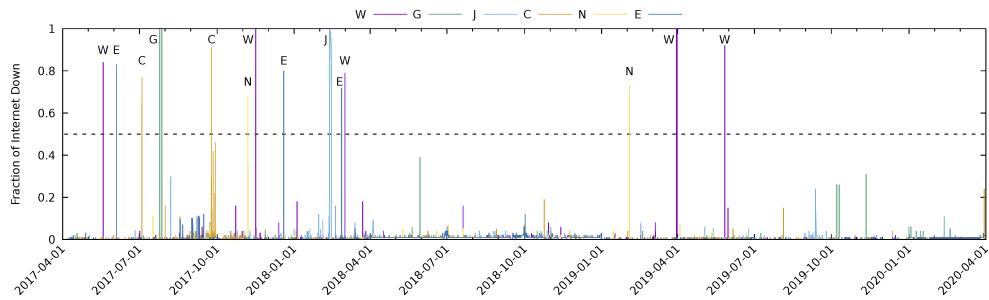
1265 In §5.7.2 we discuss evidence for country-sized islands. In 2017q3, on 8 occasions it appears
 1266 that most or all of China stopped responding to external pings. Figure 10 shows the number
 1267 of /24 blocks that were down over time, each spike more than 200k /24s, between two to
 1268 eight hours long.

1269 C.2 Longitudinal View Of Islands

1270 We first consider three years of Trinocular data (described in Appendix D.1 of [9]), from
 1271 2017-04-01 to 2020-04-01. Figure 11 shows the fraction of the Internet that is reachable as a
 1272 dotted line at the 50% threshold that Chiloe uses to detect an island (§3.2). We run Chiloe
 1273 across each VP for this period.



■ **Figure 10** Unreachable blocks over time. Large spikes are unreachability to Chinese-allocated IPv4 addresses. Dataset: A29, 2017q3.



■ **Figure 11** Islands detected across 3 years using six VPs. Datasets A28-A39.