

# What Is The Internet? (Considering Partial Connectivity)

Technical Report: arXiv:2107.11439v2

released 2021-07-23, updated 2022-05-24

Guillermo Baltra

University of Southern California  
ISI and CS Dept.  
Marina del Rey, California, USA  
baltra@isi.edu

John Heidemann

University of Southern California  
ISI and CS Dept.  
Marina del Rey, California, USA  
johnh@isi.edu

## ABSTRACT

The Internet was originally defined as “a collection of interconnected networks”. While this definition helps us understand what the Internet is, it is silent on when the Internet is *not*. We provide a *testable* definition of the Internet to clarify where the Internet “ends”: disconnection when a country or an ISP secedes; persistent partial connectivity when major ISPs refuse to exchange traffic, isolating their customers; clarifying corner cases around carrier-grade NAT, unrouted public IP addresses, and interpreting conflicting observations from systems that detect Internet outages. Our definition identifies *peninsulas* of persistent, partial connectivity, and clarifies that outages are *islands*, with internal connectivity that is partitioned from the main Internet. Our definition is conceptual, defining an ideal asymptote of connectivity, but it enables new algorithms that provide an operational estimate of the number of size of peninsulas and islands. We use these algorithms to reinterpret data from two existing measurement systems, one covering 5 million /24 IPv4 networks and the other with 10k observers. A key result is that peninsulas are about as common as outages, newly clarifying the importance of this long-observed problem. We examine root causes, showing that most peninsula events (45%) are transient routing problems, but a few long-lived peninsulas events (7%) account for 90% of all peninsula time, suggesting country- or AS-level policy choices that last weeks or more. Finally, our definition confirms the international nature of internet: no single country can unilaterally claim to be “the Internet”, but countries can chose to leave. With islands and peninsulas, our definition helps clarify the spectrum from partial reachability to outages in prior work.

## 1 INTRODUCTION

What *is* the Internet?

An “internetwork” was first used to describe a use of an early version of TCP, but without definition [15]. The first definition was “A collection of interconnected networks is

an internet”, with the ARPAnet and X.25 as two examples of internets [57]. The Federal Networking Council explicitly defined “Internet” in 1995 as (i) a global address space, (ii) supporting TCP/IP and its follow-ons, that (iii) provides services [30]. More recent work considers DNS [41] and IPv6. Such technical details are unimportant to many laypeople, who often blur the Internet with applications: to many, the World-Wide Web, Facebook, or their mobile phone is their “Internet”.

Yet the notion of a globally unique “Internet” today faces new challenges. IPv6 was proposed as a replacement for IPv4, and after 20 years of development it is an important second network. (As of December 2021, accounting for about 35% of Google’s users [34].) Others have proposed separate networks for political reasons: In 2019, Russia introduced the “sovereign Internet” law granting government wide-ranging powers to restrict traffic or physically disconnect “in an emergency” [20, 53, 61]. China has had strong views on what is allowed on their domestic Internet behind the Great Firewall [2, 3]. In 2020, Huawei suggested a “new Internet” as a set of protocols [29]. A definition would help give context to these proposals, as we explore in §2.1

But such grand changes aside, what is the Internet today? Most users access the Internet from mobile phones, with most behind Network Address Translation (NAT) devices [73], so they use IP but without a public address. Typical security recommendations mandate firewalls, preventing general addressing. And efforts such as the Interplanetary Internet [10, 42] and the Internet-of-Things seek to bring “the Internet” into space or into embedded devices.

If the Internet is networks that interconnect, then persistent failures in such interconnection are a flaw. Today’s Internet consists of many public and private companies that agree to exchange traffic through peering, either as a customer buying service from a provider, or without cost through a *settlement-free* peering. Yet disputes over peering have sometimes resulted in serious congestion [6], and even long-term

partial unreachability [45]. This unevenness has been recognized and detected experimentally [23] and other systems detect and route around partial unreachability [1, 43, 44]

The primary contribution of this paper is to define “the Internet”: *the Internet is the connected component of more than 50% of the active, public IP addresses that can reach each other* (§2). Prior definitions [15, 30, 57] distinguished the Internet from alternatives at the time, and our definition captures their idea of a *single, global Internet* (actually two, one per v4 and v6 address space). However, we provide a *testable* definition that identifies both what is and what is not part of the Internet. This property allows us to answer today’s questions about who “keeps” the name Internet if a nation or group secede. Partial reachability was first exploited in 2001 [1, 43, 44], and others observed routing transients [11]. Our definition provides the first approach to quantifying this phenomena, and it allows us to settle confusing signals and results in existing outage detection systems [36, 58, 63, 69, 70]. Our definition helps our understanding of persistent peering disputes, large-scale firewalls, and carrier-grade NAT. Although theoretical (one cannot observe from all addresses, §2), it defines an asymptote against which operational measurements maybe tested, helps us understand partial connectivity, and is not dependent on assertions of authority.

Our second contribution is to develop new algorithms (§3) that identify types of network fragmentation that underlie this definition. The first algorithm, *Taitao*, detects *peninsulas*: when a network can reach some parts of the Internet, but not others. Peninsulas result from peering disputes or long-term firewalls. Second, *Chiloe*, detects *islands*, networks that have internal connectivity but are cut off from the Internet as a whole. Our algorithms reinterpret data from two existing measurement systems that cover millions of IPv4 /24 blocks. To this existing data we add new algorithms, identifying several interesting events (§5), and adding new, independent traceroutes to validate our results (§4).

Our third contribution is to use these algorithms to understand reachability problems in the current IPv4 Internet (§5). A key result is to show that *peninsulas are as common as outages*, and that thousands of /24 IPv4 blocks are part of peninsulas lasting a month or more. This result helps establish the scope of existing detour routing systems that exploit partial reachability [1, 11, 44]. It also informs corner cases in outage detection systems [36, 58, 63, 69, 70] (§C). Measurement allows us to study root causes, and we show that peninsula events (45%) are transient routing problems, but most observations of peninsulas (90% of all peninsula time) are due to a few (7%), long-lived events suggesting country- or AS-level policy choices. Finally, it provides a technical perspective on a number of political, economic, and technical challenges to the Internet (§5.9).

All of the data used (§3.1) and created [4] in this paper is available at no cost. We review ethics in detail in §A, but our bulk analysis of IP address does not associate them with individuals. Our work was IRB reviewed and identified as non-human subjects research (USC IRB IIR00001648).

This technical report was first released in July 2021. In May 2022 it was updated with several additions: More careful discussion in §2.1 about why defining the Internet matters, a more careful definitions in §2.2 and §2.3, new information about island durations §5.7 and sizes §5.8, expanded applications in §3.5 and §5.9 and §5.10, considerable additional details and supporting data in appendices, and many writing improvements.

## 2 HOW DO WE DEFINE THE INTERNET?

While the definitions in §1 are helpful, today’s challenges impose two new requirements: First, a definition should be both *conceptual* and *operational* [25]. Our conceptual definition in §2.2 articulates *what* we would like to observe. This definition also must be operationalizable—we describe in §3 *how* actual measurement systems can estimate this value. While the conceptual definition can never be completely achieved, it defines a limit implementations can approach (§5.1). We find prior definitions too vague to operationalize.

Second, a definition should define both sufficient *and* necessary conditions to be part of the Internet, and should define properties the Internet must have (*sufficient* conditions, like TCP), but not all requirements (*necessary* conditions). Our definition should identify not only what could be part of the Internet, but also when something no longer qualifies.

### 2.1 Why Does Defining the Internet Matter?

These requirements arise due to stressors on today’s Internet from its increasing economic and political importance.

Questions of *Internet sovereignty* have brought multiple governments to assert control over the Internet, or at least their portion. In 2009, some suggested the U.S. should have an Internet “kill switch” [67]. In 2019, Russia introduced the “sovereign Internet” law with switch-off capabilities [20, 53, 61]. Since the 2000s a number of countries have created and grown nation-level firewalls and access control, either for content moderation [2, 3] or to disconnect during political unrest [21]. What happens to the Internet if a major portion secedes and chooses to operate independently? Are there now *two* Internets? If not, which part is “the” Internet?

While the intersection of national interests and the Internet is necessarily political, we define technical bounds on the outcomes. We show that no single country can unilaterally “take” the Internet (§5.10), and define islands of disconnection.

*Economic disputes* between companies that operate the Internet have stressed a unified Internet with long-term peering disputes. On multiple occasions, peering disputes resulted in persistent congestion between parts of the Internet [6, 23]. Peering disputes between Tier-1 ISPs (those with default-free routing) sometimes result in the long-term inability of parts of the Internet to reach to other parts [45]. When two Tier-1 ISPs cannot reach a business agreement to exchange traffic (such as if they cannot agree on a price), then their customers cannot reach each other. While both ISPs are part of “the Internet”, what does it mean when portions of the Internet see persistent unreachability?

Our definition enables new measurements (see §3) that allow us to quantify partial connectivity with peninsulas. We hope that measurements will provide the “sunlight” to illuminate and motivate resolution of what today are private business decisions between ISPs.

*Full allocation of the IPv4 address space and transition to IPv6* is a third stress. Given limited IPv4, many users access the Internet through NAT, sometimes in multiple layers. Some private networks today exceed designated private address space [5]. Are computers that cannot reach each other part of the Internet? Does it matter when a cloud provider has more private addresses than the public IPv4 Internet? How does the IPv6 transition change our view of the Internet?

Our definition helps clarify the role of the Internet as it evolves to heavily NAT use in IPv4 and transitions to IPv6. We consider NAT and take as an epistemological axiom that there should be *one Internet*, or a clear statement that a single Internet no longer exists.

Finally, *conflicting results in observations of Internet outages* challenge multiple independent measurement systems [36, 58, 63, 69]. Our definition and algorithms help such systems by showing that outages are not always binary, quantifying peninsulas as partial connectivity.

## 2.2 The Internet: A Conceptual Definition

We define the Internet as *the connected component of at least 50% of active, public IP addresses that can reach each other*. This conceptual definition gives *two* Internets, one for the IPv4 address space and one for IPv6. We give our reasoning for this definition below.

This definition follows from the terms “interconnected networks”, “IP protocol”, and “global address space” used in informal definitions—they all share the common assumption that two computers on the Internet should be able to communicate directly with each other at the IP layer.

We formalize “an agreement of networks to interconnect” by considering reachability over public IP addresses: addresses  $x$  and  $y$  are interconnected if traffic from  $x$  can reach

$y$  and vice versa (that is:  $x$  and  $y$  can reach each other). Networks are groups of addresses that can reach each other.

**Why More than 50%?** We require that the Internet includes more than 50% of active addresses to reflect the principle that there is *one* Internet. We believe there should be a well-defined Internet even if a major nation (or group of nations) chose to secede. A majority defines a unique, unambiguous partition that keeps the Internet.

This definition suggests that it is possible for the Internet to fragment: if the current Internet breaks into three disconnected components when none has a majority of active addresses. Such a result would end a single, global Internet.

**Why all and active addresses?** In each of IPv4 and IPv6 we consider all addresses equally. The Internet is global, and was intentionally designed without a hierarchy [16]. Our definition should not create a hierarchy or designate special addresses by age or importance, consistent with trends towards Internet decentralization [24].

We define *active* addresses as blocks that are reachable, as defined below. Our goal is to exclude the influence of large allocated but unused space. Large unused space is present in IPv4 legacy /8 allocations and in large new IPv6 allocations.

**Reachability with Protocols and Firewalls:** This conceptual definition allows for different definitions of reachability. Reachability can be tested through measurements with specific protocols, such as ICMP echo request (pings), or TCP or UDP queries. Such a test will result in an operational realization of our conceptual definition. Particular tests will differ in how closely each approaches the conceptual ideal. In §5.1 we examine how well one test converges.

Our conceptual definition considers potential reachability, but firewalls complicate operationally measuring this potential by blocking protocols or sources by policy, sometimes conditionally or unidirectionally. Thus different protocols or times might give different answers, and one could define broad reachability with any protocol in a firewall-friendly manner, or narrowly. Measurement allows us to evaluate policy-driven unreachability in §5.5.

Our use of IPv4 and ICMP echo requests (§3.1) follows prior work comparing alternatives [8, 26, 58] to show coverage is good and generally avoids rate limiting [37]).

**Why reachability and not applications?** Users care about applications, and a user-centric view might emphasize availability of HTTP or Facebook rather than IP. We recognize this attention, but intentionally measure reachability at the IP layer as a more fundamental concept. IP has changed only twice since 1969 with IPv4 and IPv6, but dominant applications ebb and flow, and important applications often extend beyond the Internet. (E-mail has been transparently relayed to UUCP and FidoNet, and the web to pre-IP mobile devices with WAP.) Future work may look at applications, but we see IP-level reachability as an essential starting point.

**Why bidirectional reachability?** Most computers today access the Internet indirectly through Network Address Translation. While such computers are useful as Internet clients, our requirement for bidirectional reachability excludes them from being fully “on” the Internet. They cannot provide services or participate in peer-to-peer protocols without work-arounds such as public-IP STUN server [68].

Similarly, services may be operated as many computers behind a single public IP address with load balancing or IP anycast [56], perhaps with cloud-based address translation [35]. Computers with only application-level availability are also not fully part of the Internet.

### 2.3 The Internet Landscape

Our definition of the Internet highlights the Internet’s “rough edges”. Using our conceptual definition of the Internet as the fully connected component (§2.2), we identify three specific problems: an address  $a$  is a *peninsula* when it has partial connectivity to the Internet, an *island* when it cannot reach any of the Internet, and an *outage* only when it is off.

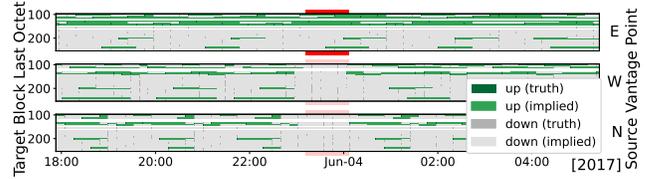
**2.3.1 Outages.** A number of groups have examined Internet outages [36, 58, 63, 69]. These systems observe the IPv4 Internet and identify networks that are no longer reachable—they have left the Internet. Often these systems define outages operationally (network  $x$  is out because none of our Vantage Points (VPs) can reach it). Conceptually, an outage is when all computers in a block are off, such as due to a power outage. If the computers or their network are on but cannot reach the Internet, we consider them islands, defined next.

**2.3.2 Islands: Isolated Networks.** An *island* is a group of public IP addresses that are partitioned from the Internet, but can communicate among themselves. Both outages and islands are unreachable from an external VP, but with islands the computers are still active and talking among themselves.

Islands occur when an organization that has a single connection to the Internet loses its router or link to its ISP. A single-office business may become an island after a router failure, yet staff may use a webserver with them in the office even though they are unable to surf the public web. In the smallest case, an island may be a single address that can only ping itself, that is, an *address island*.

We suspect that most outages are actually temporary islands. The conditions are identical from the outside, but can be distinguished by an observer within.

**A Small Island:** Figure 1 shows an example of an island we have observed. In this graph, each strip shows a different VP’s view of the last 156 addresses from the same IPv4 /24 block over 12 hours, starting at 2017-06-03t23:06Z. In each strip, the darkest green dots show positive responses of that



**Figure 1: A one-hour island (the middle in red) where block 65.123.202.0/24 is reachable from VP E (middle bar) but not the other 5 VPs (top and bottom). Dataset: A28, 2017q2.**

address to an ICMP echo request (a “ping”) from that observer, and medium gray dots indicate a non-response to a ping. We show inferred state as lighter green or lighter gray until the next probe. We show 3 of the 6 VPs, with probes intervals of about 11 minutes (for methodology, see §3.1).

The island is indicated by the red bar in the middle of the graph, where VP E continues to get positive responses from several other addresses (the continuous green bars along the top). By contrast, the other 5 VPs (2 VPs here, others in §E.2) show many non-responses during this period. For this whole hour, VP E and this network are part of an island, cut off from the rest of the Internet and the other VPs.

Typically, a company losing Internet access would be called an Internet *outage*, not an island. (In fact, with current use of cloud-hosted services, loss of Internet may well stop all work in the company.) We have also seen country-sized islands (in §E.1 for space).

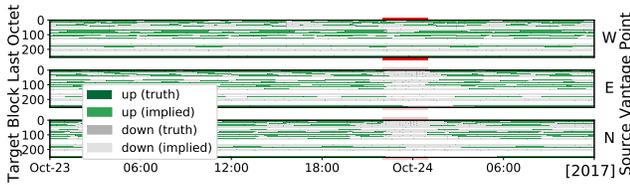
**2.3.3 Peninsulas: Partial Connectivity.** While outages happen and create islands, a more pernicious problem is *partial* connectivity, when one can reach some destinations, but not others. We call a group of public IP addresses with partial connectivity with the Internet a *peninsula*<sup>1</sup>. The presence of peninsulas has been recognized for nearly twenty years, with overlay networks demonstrated to route around them in RON [1], Hubble [43], and later LIFEGUARD [44].

Peninsulas occur when a multi-homed network has outages or peering disputes upstream, or due to firewalls.

**Examples in IPv6:** An example of a persistent peninsula is the IPv6 peering dispute between Hurricane Electric (HE) and Cogent. These two Tier-1 ISPs do not peer in IPv6, and as Tier-1 ISPs, they are also unwilling to send IPv6 to each other through another party (the “no valley” routing policy). This problem was noted in 2009 [45] and is visible as of June 2020 in DNSMON [65] as a few percent of persistent unreachability in most Root DNS server’s IPv6.

We see unreachability between HE and Cogent users in IPv6 with traceroutes from looking glasses [18, 28] in one

<sup>1</sup>We consider it a peninsula because one cannot route directly between two points, but instead must detour through a third party.



**Figure 2: A block (80.245.176.0/24) showing a 3-hour peninsula accessible only from VP W (top bar) and not from the other 5 VPs (only 2 shown). Dataset: A30, 2017q4.**

to DNS in the other (HE at 2001:470:20::2 and Cogent at 2001:550:1:a::d). Neither can reach their neighbor’s server, but both reach their own. We do not see this problem on IPv4 (HE at 74.82.42.42 and Cogent at 66.28.0.14).

Other IPv6 dispute examples are Cogent with Google [59], and Cloudflare with Hurricane Electric [31]. Peering disputes are often the result of traffic imbalance and disagreements about a settlement-free or customer/provider relationship.

**An Example in IPv4:** We next explore a real-world example of partial reachability to several Polish ISPs that we found with our algorithms. On 2017-10-23, for a period of 3 hours starting at 22:02Z, five Polish Autonomous Systems (ASes) had 1716 blocks that were unreachable from five VPs while the same blocks remained reachable from a sixth VP.

Before the peninsula, the blocks that became partially unreachable all received service through Multimedia Polska (AS21021, or *MP*), via Cogent (AS174), with an alternate path through Tata (AS6453). When the peninsula occurred, traffic continued through Cogent but was blackholed; it did not shift to Tata (see §D). One VP (W) could reach MP through Tata for the entire event, proving MP was connected. After 3 hours, we see a burst of BGP updates (more than 23k), making MP reachable again from all VPs.

To show how our algorithms detect this, Figure 2 shows responses for one block. In this case the top VPs can reach the block always, but the lower two are unreachable (all address gray) for 3 hours.

We can confirm this peninsula with additional observations from traceroutes taken by CAIDA’s Archipelago [12] (Ark). During the event we see 94 unique Ark VPs attempted 345 traceroutes to the affected blocks. Of the 94 VPs, 21 VPs (22%) have their last responsive traceroute hop in the same AS as the target address, and 68 probes (73%) stopped before reaching that AS. The remaining 5 VPs were able to reach the destination AS for some probes, while not for others. (Sample traceroutes are in §D.)

Although we do not have a root cause for this peninsula from network operators, large number of BGP Update messages suggests a routing problem. In §5.4 we show peninsulas are mostly due to policy choices.

### 3 METHODOLOGY

We use observations from multiple, independent VPs to detect partial outages and islands (from §2) with our two new algorithms: *Taitao* to detect peninsulas, and *Chiloe*, to detect islands (named after Patagonian geography).

#### 3.1 Data Sources

We use publicly available data from three systems: USC Trinocular [58], RIPE Atlas [66], and UCSD’s Archipelago [13].

Our algorithms use data from Trinocular [58] because it is available at no cost [76], provides data since 2014, and covers most of the responsive IPv4 Internet [7]. Briefly, Trinocular watches about 5M out of 5.9M responsive IPv4 /24 blocks. In each probing round of 11 minutes, it sends up to 15 ICMP echo requests (pings), stopping early if it proves the block is reachable. It interprets the results using Bayesian inference, and merges the results from six geographically distributed VPs. VPs are in Los Angeles (W), Colorado (C), Tokyo (J), Athens (G), Washington, DC (E), and Amsterdam (N). In §C.2 we show they are topologically independent. Our algorithms should work with other active probing data as future work.

We use RIPE Atlas [66] to study islands in §3.4. As of 2022, it has about 12k VPs, distributed globally in over 3572 different IPv4 ASes. Atlas VPs carry out both researcher-directed measurements and periodic scans of DNS servers. We use Atlas scans of DNS root servers in our work.

We validate our results using CAIDA’s Ark [13], and use AS numbers from Routeviews [49].

We generally use recent data, but in some cases we chose older data to avoid known problems in measurement systems. We show our results are robust to other time periods in §F. We use Trinocular measurements for 2017q4 because this time period had six active VPs, allowing us to make strong statements about how multiple perspectives help. We use 2020q3 data in §5.4 because Ark observed a very large number of loops in 2017q4. Problems with different VPs reduced coverage for 2019 and 2020, but we verify and find quantitatively similar results for 2020 data in §F).

We list sources of all datasets we use in Table 9 in §B.

#### 3.2 Taitao: a Peninsula Detector

Peninsulas occur when portions of the Internet are reachable from some locations and not others. Peninsulas can be observed when two VPs disagree on block reachability. With multiple VPs, any state other than all-up or all-down suggests a peninsula.

Detecting peninsulas presents three challenges. First, we do not have VPs everywhere. If all VPs are on the same “side” of a peninsula, their reachability agrees even though other potential VPs may disagree. Second, VP observations are not synchronized and are spread over an 11-minute probing interval, so we expect that different VPs will make observations at slightly different times. Thus two correct observations may see before and after a network change, producing a false agreement or disagreement. Third, a VP may be suffering connectivity problems, such as being in an island.

We identify peninsulas by detecting disagreements in block state by comparing valid VP observations that occur at about the same time. Since probing rounds occur every 11 minutes, we compare measurements within an 11-minute window. This approach will see peninsulas that last at least 11 minutes, but may miss briefer ones, or peninsulas where VPs are not on “both sides”.

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

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

When only one VP reaches a block, that block can be either a peninsula or an island. We require more information to distinguish them, as we describe in §3.4.

### 3.3 Country-Level Peninsula Detection

Taitao detects peninsulas based on differences in observations. Long-lived peninsulas are likely intentional, from policy choices. One policy is filtering based on national boundaries, possibly to implement legal requirements about data sovereignty or economic boycotts.

We identify country-specific peninsulas as a special case of Taitao where a given destination block is reachable (or unreachable) from only one country, persistently for an extended period of time. (In practice, the ability to detect country-level peninsulas is somewhat limited because the only country with multiple VPs in our data is the United States. However, we augment non-U.S. observers with data from other non-U.S. sites such as Ark or RIPE Atlas.)

A country level peninsula occurs when *all* available VPs from the same country as the target block successfully reach the target block and all available VPs from different countries fail. Formally, we say there is a country peninsula when the set of observers claiming block  $b$  is up at time  $i$  is equal to  $O_{i,b}^c \subset O_{i,b}$  the set of all available observers with valid observations at country  $c$ .

$$O_{i,b}^{up} = O_{i,b}^c \quad (2)$$

### 3.4 Chiloe: an Island Detector

According to our definition in §2.3.2, islands occur when the Internet is partitioned, and the smaller component (that with less than half the active addresses) is the island. Typical islands are much, much smaller.

We can find islands by looking for networks that are only reachable from less than half of the Internet. However, to classify such networks as an island and not merely a peninsula, we need to show that it is partitioned. Without global knowledge, it is difficult to prove disconnection. In addition, if islands are partitioned from VPs, we cannot tell an island, where a part of the Internet is disconnected but still active inside, from an outage, where a part of the Internet is disconnected and also cannot communicate internally.

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

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

$$0 \leq |B_{i,o}^{up}| \leq |B_{i,o}^{dn}| \quad (3)$$

This method is independent from measurement systems, but is limited to detecting islands that contain VPs. We evaluate two systems with thousands of VPs in §5.6. Also, because observation is not instantaneous, we must avoid confusing short-lived islands with long-lived peninsulas. For islands lasting longer than an observation period, we also require  $|B_{i,o}^{up}| \rightarrow 0$ . When  $|B_{i,o}^{up}| = 0$ , then we have an address island.

### 3.5 Algorithm Applications

**Practical: Cleaning Data.** Problems near network observers can skew observations and must be detected and removed. We currently use island detection to remove local outages when using VPs for detection of Covid-work-from-home [71].

**Understanding Risk:** Our work also helps clarify that Internet reachability is not binary, but often partial. We explore this issue in §5; one key result is that users see peninsulas as often as outages (§5.1). It helps clarify prior studies of Internet outages [36, 58, 63, 69, 70] (more detail is in §C).

**Theoretical: Who Has the Internet?** We explore this question in §5.9 and §5.10.

## 4 VALIDATING OUR APPROACH

We next validate our approaches. We compare Taitao peninsulas against independent data (§4.1) and examine persistent

country-level peninsulas (§4.2). We then compare Chiloe’s island detection with external observers (§4.3).

#### 4.1 Can Taitao Detect Peninsulas?

We compare Taitao detections from 6 VPs to independent observations taken from more than 100 VPs in CAIDA’s Ark [13]. This comparison is challenging, because both Taitao and Ark are operational systems with imperfect results, and because they differ in probing frequency, targets, and method. Neither defines perfect ground truth; but agreement suggests likely truth, and we discuss possible causes of disagreements.

Although Ark probes targets much less frequently than Trinocular, Ark makes observations from 171 global locations, so it provides a fresh perspective. Ark’s traceroutes also allows us to assess *where* peninsulas begin. We expect to see a strong correlation between Taitao peninsulas and Ark observations. (We considered RIPE Atlas as another external dataset, but its coverage is sparse, while Ark covers all /24s.)

**Identifying comparable blocks:** We study 21 days of Ark observations from 2017-10-10 to -31. Ark covers all networks with two strategies. With team probing, 40 VPs traceroute to every routed /24 about once per day. For prefix probing, about 35 VPs send traceroutes to .1 addresses of all routed /24s every day. We use both types of data: all three teams and all available prefix probing VPs, and we group results by /24 block of the traceroute’s target address.

Ark differs from Taitao’s Trinocular input in three ways: the target is a random address or the .1 address in each block; it uses traceroute, not ping; and it probes blocks daily, not every 11 minutes. Comparisons must consider these differences, since Ark traceroutes will sometimes fail when a simple ping succeeds. First, Trinocular uses of likely-to-respond addresses, while Ark does not, so Trinocular has a higher response rate. Second, Ark’s traceroutes terminate due to four reasons: *success* in reaching target address, ICMP *unreachable* message to the target address, *loop* in the path, or *gap* limit exceeded. We discard gap outcomes, since gaps indicate problems on the path and may hide an endpoint that would be reachable if it were directly pinged.

To correct for differences in target addresses, we must avoid misinterpreting a block as unreachable when the block is online but Ark’s target address is not, we discard traces sent to never-active addresses (those not observed in 3 years of complete IPv4 scans), and blocks for which Ark did not get a single successful response. (Even with this filtering, dynamic addressing means Ark still sometimes sees unreachables.)

To correct for Ark’s less frequent probing, we compare Trinocular down-events that last 5 hours or more. Ark measurements are much less frequent (once every 24 hours) than Trinocular’s 11-minute reporting, so short Trinocular events often have no overlapping Ark observations. To confirm

agreements or conflicting reports from Ark, we require at least 3 Ark observations within the peninsula’s span of time.

We filter out blocks that show frequent transient changes or show signs of network-level filtering. We define the “reliable” blocks that we keep as blocks that report as up at least 85% of the quarter from each of the 6 Trinocular VPs. We also discard as flaky blocks with frequently inconsistent responses across VPs. (We consider more than 10 combinations of VP as frequently inconsistent.) For the 21 days, we find 4M unique Trinocular /24 blocks, and 11M Ark /24 blocks, making 2M blocks in both available for study.

**Results:** Table 1 provides details and Table 2 summarizes our interpretation. Here dark green indicates true positives (TP): when (a) either both Taitao and Ark show mixed results, both indicating a peninsula, or when (b) Taitao indicates a peninsula (1 to 5 sites up but at least one down), Ark shows all-down during the event and up before and after. We treat Ark in case (b) as positive because the infrequency of Ark probing (one probe per team every 24 hours) means we cannot guarantee VPs in the peninsula will probe responsive targets in time. Since peninsulas are rare, so too are true positives, but we see 184 TPs.

We show *true negatives* as light green and neither bold nor italic. In almost all of these cases (1.4M) both Taitao and Ark both reach the block, agreeing. Because of dynamic addressing [55], many Ark traceroutes end in a failure at the last hop (even after we discard never-reachable). We therefore count this second most-common result (491k cases) as a true negative. For the same reason, we include the small number (97) of cases where Ark reports conflicting results and Taitao is all-up, assuming Ark terminates at an empty address. We include in this category, the 90 events where Ark is all-down and Trinocular is all-up. We attribute Ark’s failure to reach its targets to infrequent probing.

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

Finally, yellow italics shows cases where a Taitao peninsula is a *false positive*, since all Ark probes reached the target block. This scenario 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 with independent VPs, five of six observers have working paths). Discarding these cases we get 40 (orange), a *loose* 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 good, but with some room for improvement.

		Ark			
		Sites Up	Conflicting	All Down	All Up
Trinocular	Conflicting	1	20	6	15
		2	13	5	11
		3	13	1	5
		4	26	4	19
		5	83	13	201
Trinocular	Agree	0	6	97	6
		6	491,120	90	1,485,394

**Table 1: Trinocular and Ark agreement table. Dataset A30, 2017q4.**

		Ark		
		Peninsula	Non Peninsula	
Taitao	Peninsula	184	251 ( <i>strict</i> )	40 ( <i>loose</i> )
	Non Peninsula	12	1,976,701	

**Table 2: Taitao confusion matrix. Dataset A30, 2017q4.**

		Ark			Total
		U.S. VPs	Domestic Only	≤ 5 Foreign	
Trinocular	WCE	211	171	47	429
	WcE	0	5	1	6
	WeE	0	1	0	1
	wCE	0	0	0	0
	Wce	3	40	11	54
	wcE	0	4	5	9
	wCe	0	1	1	2
	Marginal distr.	214	222	65	501

**Table 3: Trinocular U.S.-only blocks. Dataset A30, 2017q4.**

		Trinocular		
		Blk Island	Addr Island	Peninsula
Chiloe	Island	2	19	2
	Peninsula	0	8	566

**Table 4: Chiloe confusion matrix, events between 2017-01-04 and 2020-03-31. Datasets A28 through A39.**

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	<b>235,170</b>	<b>133,728</b>	<b>61,392</b>	<b>307,506</b>
6	967,888	812,430	238,182	1,542,136

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

Sites	Events	Per Year
W	5	1.67
C	2	0.67
J	1	0.33
G	1	0.33
E	3	1.00
N	2	0.67
All (norm.)	14	4.67 (0.78)

**Table 6: Islands detected from 2017q2 to 2020q1**

## 4.2 Detecting Country-Level Peninsulas

Next, we verify detection of country-level peninsulas (§3.3). We expect that legal requirements sometimes result in long-term network unreachability. For example, blocking access from Europe is a crude way to comply with the EU’s GDPR [74].

Identifying country-level peninsulas requires multiple VPs in the same country. Unfortunately the source data we use only has multiple VPs for the United States. We therefore look for U.S.-specific peninsulas where only these VPs can reach the target and the non-U.S.-VPs cannot, or vice versa.

We first consider the 501 cases where Taitao reports that only U.S. VPs can see the target, and compare to how Ark VPs respond. For Ark, we follow §4.1, except retaining blocks with less than 85% uptime. We only consider Ark VPs that are able to reach the destination (that halt with “success”). We note blocks that can only be reached by Ark VPs within the same country as domestic, and blocks that can be reached from VPs located in other countries as foreign.

In Table 3 we show the number of blocks that uniquely responded to all U.S. VP combinations during the quarter. We contrast these results against Ark reachability.

True positives are when Taitao shows a peninsula responsive only to U.S. VPs and nearly all Ark VPs confirm this result. We see 211 targets are U.S.-only, and another 171 are available to only a few non-U.S. countries. The specific combinations vary: sometimes allowing access from the U.K., or Mexico and Canada. Together these make 382 true positives, most of the 501 cases. Comparing all positive cases, we see a

very high precision of 0.99 (382 green of 385 green and red reports)—our predictions are nearly all confirmed by Ark.

In yellow italics we show 47 cases of false positives where more than five non-U.S. countries are allowed access. In many cases these include many European countries. Our recall is therefore 0.89 (382 green of 429 green and yellow true country peninsulas).

In light green we show true negatives. Here we include blocks that filter one or more U.S. VPs, and are reachable from Ark VPs in multiple countries, amounting to a total of 69 blocks. There are other categories involving non-U.S. sites, along with other millions of true negatives, however, we only concentrate in these few.

In red and bold we show three false negatives. These three blocks seem to have strict filtering policies, since they were reachable only from one U.S. site (W) and not the others (C and E) in the 21 days period.

## 4.3 Can Chiloe Detect Islands?

Chiloe (§3.4) detects islands when a VP within the island can reach less than half the rest of the world. When less than 50% of the network replies, it means that the VP is either in an island (for brief events, or when replies drop near zero) or a peninsula (long-lived partial replies).

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 define ground truth at a block level granularity—if VP  $x$  can reach its own block when  $x$  believes to be in an

island, while other external VPs can't reach  $x$ 's block, then  $x$ 's island is confirmed. On the other hand, if an external VP can reach  $x$ 's block, then  $x$  is not in island, but in a peninsula. In §C.2 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, but of course a perfect identification of island or peninsula requires instant, global knowledge and so cannot be measured in practice.

We take 3 years worth of data from each of the six Trinocular VPs. Since Trinocular measures blocks asynchronously every 11 minutes, we use 11 minute timebins as our snapshot of the Internet. We ignore cases where the VP can access 95% or more of the Internet.

In Table 4 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 ground-truth 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.

The 566 non-island events (true negatives) are when more than 5% but less than 50% of the Internet was inaccessible from a single VP. In each of these cases, one or more other VPs were able to reach the affected VP's block, showing they were not an island (although perhaps a peninsula). We omit the very frequent events when less than 5% of the network is unavailable from the VP from the table, although they too are true negatives.

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

## 5 QUANTIFYING ISLANDS AND PENINSULAS

We next apply our approach to the Internet. For peninsulas: how often do they occur (§5.1), how long do they last (§5.2), and how big are they (§5.3)? These evaluations characterize how effective systems using overlay routing [1, 43, 44] are. We also look at peninsula location by ISP (§5.4) and country (§5.5). Finally, we look at island frequency (§5.6) and the implications of country-level internet secession (§5.10).

### 5.1 How Common are Peninsulas?

We next estimate how common peninsulas are in the Internet in two ways. First, we directly measure the visibility of

peninsulas in the Internet by summing the duration of peninsulas as seen from our six VPs. We also confirm the accuracy of this estimate by evaluating its convergence as we vary the number of VPs—more VPs show more peninsula-time, but if the result converges we predict we are approaching the limit. Second, we compare peninsula-time to outage-time, showing that, in the limit, both observes see both for about the same duration. Since outages are a recognized problem by both academia and industry due to service downtime [78], this demonstration that peninsulas are as common suggests they are an important new problem to address.

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

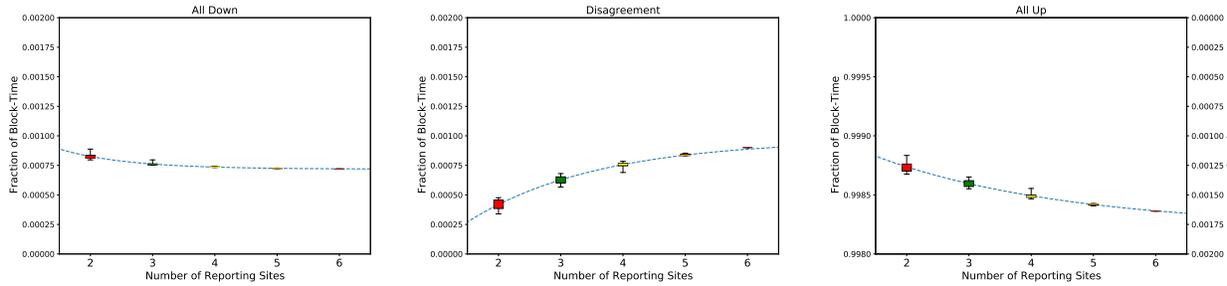
We have computed peninsula-time by evaluating Taitao over Trinocular data for 2017q4 [76]. Figure 3 shows the distribution of peninsulas measured as a fraction of block-time for an increasing number of sites. We consider all possible combinations of the six sites.

First we examine the data with all 6 VPs—the rightmost point on each graph. We see that peninsulas (the middle, disagreement graph) are visible about 0.00075 of the time. This data suggests *peninsulas are rare, occurring less than 0.1% of the time, but do regularly occur*.

**Convergence:** With more VPs we get a better view of the Internet's overall state. As more reporting sites are added, more peninsulas are discovered. That is, previous block states erroneously inferred as all up or all down, are corrected to peninsulas. All-down (left) decreases from an average of 0.00082 with 2 VPs to 0.00074 for 6 VPs. All-up (right) goes down a relative 47% from 0.9988 to 0.9984, while disagreements (center) increase from 0.0029 to 0.00045. *Outages (left) converge after 3 sites*, as shown by the fitted curve and decreasing variance. Peninsulas and all-up converge more slowly. We conclude that *a few sites (3 or 4) provide a good estimate of true outages and peninsulas*.

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

**Generalizing:** We confirm these results with other quarters in §F. While we reach a slightly different limit (in that case, peninsulas and outages appear about in 0.002 of data), we still see good convergence after 4 VPs.



**Figure 3: Distribution of block-time fraction over sites reporting all down (left), disagreement (center), and all up (right), for events longer than one hour. Dataset A30, 2017-10-06 to 2017-11-16.**

### 5.2 How Long Do Peninsulas Last?

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

To characterize peninsula duration we use Taitao to detect peninsulas that occurred during 2017q4. For *all* peninsulas, we see 23.6M peninsulas affecting 3.8M unique blocks. If instead we look at *long-lived* peninsulas (at least 5 h), we see 4.5M peninsulas in 338k unique blocks. Figure 4a examines the duration of these peninsulas in three ways: the cumulative distribution of the number of peninsulas for all events (left, solid, purple line), the cumulative distribution of the number of peninsulas for VP down events longer than 5 hours (middle, solid green line), and the cumulative size of peninsulas for VP down events longer than 5 hours (right, dashed green line).

We see that there are many very brief peninsulas (purple line): about 65% last from 20 to 60 minutes (about 2 to 6 measurement rounds). Such events are not just one-off loss, since they last at least two observation periods. These results suggest that while the Internet is robust, there are many small connectivity glitches (7.8M events).

In addition, we see some events that are two rounds (20 minutes) or shorter. Such events could be BGP transients or failures due to random packet loss.

The number of day-long or multi-day peninsulas is small, only 1.7M events (2%, the purple line). However, about 57% of all peninsula-time is in such longer-lived events (the right, dashed line), and 20% of time is in events lasting 10 days or more, even when longer than 5 hours events are less numerous (compare the middle, green line to the left, purple line). Events lasting a day are long-enough that they can be

debugged by human network operators, and events lasting longer than a week are long-enough that they may represent policy disputes. Together, these long-lived events suggest that there is benefit to identifying non-transient peninsulas and addressing the underlying routing problem.

### 5.3 What Sizes Are Peninsulas?

When network issues cause connectivity problems like peninsulas, the *size* of those problems may vary, from country-size (see §5.5), to AS-size, and also for routable prefixes or fractions of prefixes. We next examine peninsula sizes.

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

We compare peninsulas to routable prefixes from Routeviews [49]. We perform longest prefix match between /24 blocks and prefixes.

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

Figure 4b shows the number of peninsulas for different prefix lengths and the fraction of the prefix affected by the peninsula as a heat-map, where we group them into bins.

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

Finally, we show that *longer-lived peninsulas are likely due to routing or policy choices*. Figure 4c shows the same

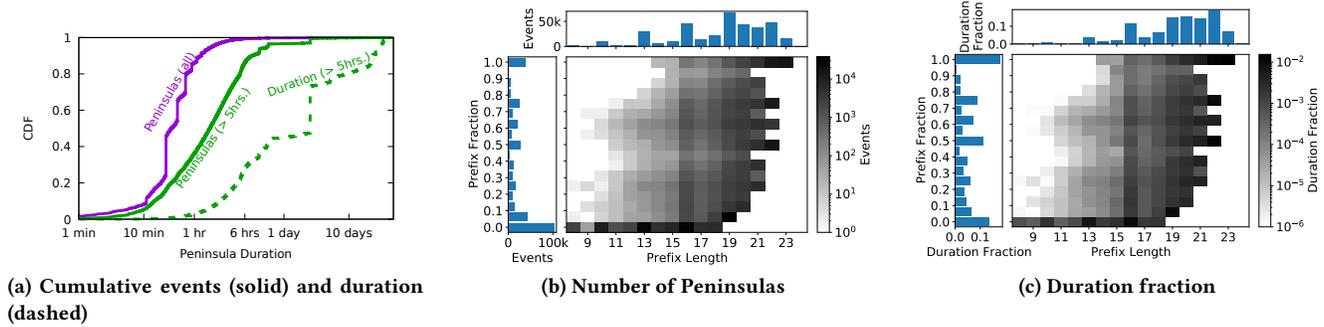


Figure 4: Peninsulas measured with per-site down events longer than 5 hours. Dataset A30, 2017q4.

data source, but weighted by fraction of time each peninsula contributes to the total peninsula time during 2017q4. Here the larger fraction of weight are peninsulas covering full routable prefixes—20% of all peninsula time during the quarter (see left margin).

### 5.4 Where Do Peninsulas Occur?

Firewalls, link failures, and routing problems cause peninsulas on the Internet. These can either occur inside a given AS, or in upstream providers.

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 find where these traces halt, and take note whether halting occurs *at* the target AS and target prefix, or *before* the target AS and target prefix.

For our experiment we run Taitao to detect peninsulas at target blocks over Trinocular VPs, we use Ark’s traceroutes [14] to find last IP address before halt, and we get target and halting ASNs and prefixes using RouteViews.

In Table 5 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). 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 peninsulas are policy choices.

### 5.5 Country-Level Peninsulas

Country-specific filtering is a routing policy made by networks to restrict traffic they receive. We next look into what

Industry	ASes	Blocks
ISP	23	138
Education	21	167
Communications	14	44
Healthcare	8	18
Government	7	31
Datacenter	6	11
IT Services	6	8
Finance	4	6
Building Security, Cloud, Construction, Grocery Stores, Insurance, Media	6 (1 each type)	

Table 7: U.S. only blocks. Dataset A30, 2017q4

type of organizations actively block overseas traffic. For example, good candidates to restrain who can reach them for security purposes are government related organizations.

We test for country-specific filtering (§3.3) over 2017q4 and find 429 unique U.S.-only blocks in 95 distinct ASes. We then manually verify each AS categorized by industry in Table 7. It is surprising how many universities filter by country. While not common, country specific blocks do occur.

### 5.6 How Common Are Islands?

Multiple groups have shown that there are many network outages in the Internet [36, 58, 63, 69, 70]. We have described (§2) two kinds of outages: full outages where all computers at a site are down (perhaps due to a loss of power), and islands, where the site is cut off from the Internet but computers at the site can talk between themselves. We next use Chiloe to determine how often islands occur. We study islands in two systems with 6 VPs for 3 years and 13k VPs for 3 months.

**Trinocular:** We first consider three years of Trinocular data (described in §3.1), from 2017-04-01 to 2020-04-01. We run Chiloe across each VP for this period.

Table 6 shows the number of islands per VP over this period. Over the 3 years, all six VPs see from 1 to 5 islands.

In addition, we see that islands do not always cause the *entire* Internet to be unreachable, and there are a number of cases where from 20% to 50% of the Internet is inaccessible. We believe these cases represent brief islands, since islands shorter than an 11 minute complete scan will only be partially observed. We find 12 in the 20% to 50% range, all are short, and 4 are less than 11 minutes (see §E.3 for details).

**RIPE Atlas:** For broader coverage we next consider RIPE Atlas’ 13k VPs for the three months of 2021q3 [51]. While Atlas does not scan the whole Internet, they do scan most root DNS servers every 240 s. Chiloe would like to observe the whole Internet, and while Trinocular scans 5M /24s, it does so with only 6 VPs. To use RIPE Atlas as 10k VPs, we further relax our operational definition of the Internet to consider only the 13 DNS root servers. While a large step down in size, root servers are independently operated and physically distributed, so we consider their probing a very sparse sample. Thus we have complementary datasets with sparse VPs and dense probing, and many VPs but sparse probing. In other words, to get many VP locations we relax our conceptual definition by decreasing our target list.

Figure 5a shows the CDF of the number of islands detected per RIPE Atlas VP during 2021q3. During this period, 41% of VPs observed one or no islands (solid line). To compare to Trinocular, we consider events longer than 660s with the dashed line. In the figure, 50% of VPs saw no islands, 20% see one, and the remainder see more. The annualized island rate of just the most stable VPs (those that see 0 or 1 islands) is 1.14 islands per year (a lower bound, since we exclude less stable VPs), compared to 0.78 for Trinocular (Figure 5a). We see islands are more common in Atlas, perhaps because it includes many VPs at home.

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

## 5.7 How Long Do Islands Last?

Islands can occur starting from brief connectivity losses to long standing policy changes. We next compare island duration measured across Trinocular and Atlas.

We compare the distributions of island durations observed from RIPE Atlas (left line) and Trinocular (the right line) in Figure 5b. Atlas’ frequent polling allows it to detect islands lasting seconds, while Trinocular is limited to islands of 660 s or longer, so we also show the distribution of Atlas events lasting that long or longer (middle line). All measurements follow a similar S-shaped curve, but for Trinocular, the curve is truncated at 660 s. With only 6 VPs, Trinocular sees far fewer events (14 in 3 years compared to 235k in a yearly quarter with Atlas), so the Trinocular data is quantized. In both cases, about 70% of islands are between 3000 and 7000 s.

This graph shows that Trinocular’s curve is similar in shape to Atlas-660 s, but about 2× longer. All Trinocular observers are in datacenters, while Atlas devices are at homes, so this difference may indicate that datacenter islands are rarer, but harder to resolve.

## 5.8 What Sizes Are Islands?

In §2.3 we described different sizes of islands starting from as small as an address island, as opposed to LAN- or AS-sized islands, to country-sized islands potentially capable of partitioning the Internet.

To evaluate the size of islands we count the number of hops in a traceroute sent towards a target outside the island before the traceroute fails.

We take traceroute data from RIPE Atlas VPs sent to 12 root DNS servers (ABCDEFGHIJKLM) for 2021q3 [52]. In Figure 5c in green the distribution of the number of hops when traceroute reach their target. In purple, we plot the distribution of the number of hops of traceroutes that failed to reach the target for VPs in islands detected in §5.6.

We find that most islands are small, 68% show one hop or none (address islands). We consider that islands with 10 or more hops correspond to false positives.

## 5.9 Applying the Definition to Challenges

We next explore use of the definition in several challenges to Internet operation. We suggest that these examples show the role of our definition at providing a clear boundary for “part of the Internet”. In many of these examples, technical issues have been studied, and political and economic issues considered—presence of a definition does not simplify these important factors. However, we suggest that a conceptual definition can help provide clarity in these tussles with a decentralized, independently measurable principal about where the Internet begins and ends.

**Secession and Sovereignty:** The U.S. [67], China [2, 3], and Russia [17] have all proposed unplugging from the Internet. Egypt did during Arab spring [19], and several countries do during exams [22, 27, 33, 39]. When the Internet partitions, which part is still “the Internet”? Departure of a business, ISP, or a small country would go unnoticed, but what happens if a large country or group of countries leave?

Our definition resolves this question, defining the Internet from reachability of the majority of the active, public IP addresses (§2.2). Majority uniquely provides an unambiguous, externally evaluable decision—the partition retaining 50% of prior active addresses is the Internet. A corollary we explore in §5.10 is that creation of multiple partitions can end the Internet if none retain a majority. (A plurality is insufficient.)

**Sanction:** An opposite of secession is expulsion. Economic sanctions are one method of asserting international

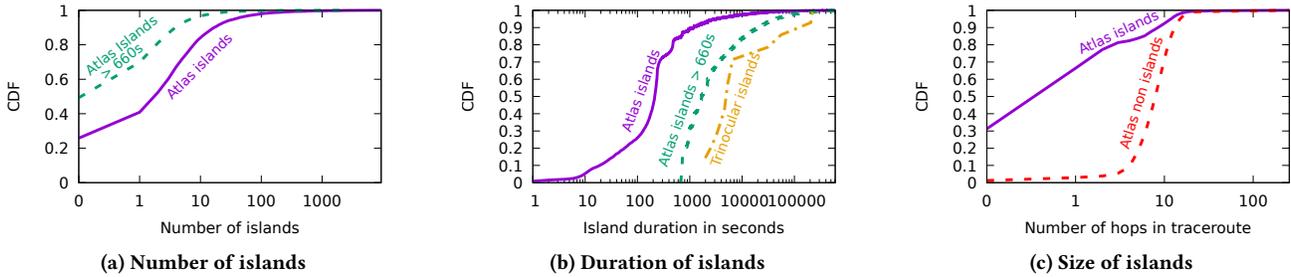


Figure 5: CDF of islands detected by Chiloe for data from Trinocular (3 years, Datasets A28-A39) and Atlas (2021q3).

influence, and events such as the Russian/ Ukrainian war in 2022 prompted several large ISPs to discontinue service to Russia [62]. De-peering does not affect reachability if transit is available through other ISPs, but it will result in a peninsula without transit. Based on §5.10, de-peering without transit from a single country cannot eject a country from the Internet. However, a coalition of multiple countries could result in unreachability from more than half the address space, which by our definition would place the affected address space outside the public Internet.

**Repurposing Special Space:** Given IPv4 full allocation, multiple parties proposed re-purposing currently allocated or reserved IPv4 space, such as parts of 0/8 (“this” network), 127/8 (loopback), 240/4 (reserved) [32]. The primary challenge against re-purposing such prefixes is that existing software and hardware prohibit use of this space, and changing them is difficult or impossible. By our definition, even an RFC designating of 240/4 as public unicast space, would not make it “part of the Internet” until implementations used by a majority of active addresses can route to it.

**IPv4 Squat Space:** IP squatting is when an organization requiring private address space beyond RFC1918 takes over allocated but currently unrouted IPv4 space [5]. Several IPv4 /8s allocated to the U.S. DoD were widely used this way [64] but were publicly routed in 2021 [72]. By our definition, such space is clearly not part of the Internet before it is publicly routed, and if more than half of the Internet is squatting on it, reclamation may be challenging.

**The IPv4/v6 Transition:** We have defined two Internets, one for IPv4 and one for IPv6. Our definition can inform when one network supersedes the other. The networks would be on par when more than half of all hosts in IPv4 are dual-homed. After that point, IPv6 would supersede IPv4 when a majority of hosts on IPv6 could no longer reach IPv4. Without current measures of IPv6, evaluation here is future work, but we believe the networks are not yet on-par, IPv6 shows the strength and limitations of our definition: on one hand, IPv6 is already economically important, making a definition

RIR	IPv4 Addresses		IPv6 Addresses			
	Active	Allocated	Active	Allocated		
AFRINIC	15M	2%	121M	3.3%	9,661	3%
APNIC	223M	33%	892M	24.0%	88,614	27.8%
China	112M	17%	345M	9.3%	54,849	17.2%
ARIN	150M	22%	1,673M	45.2%	56,172	17.6%
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 8: RIR IPv4 hosts and IPv6 /32 allocation [40, 54]

irrelevant. However, we suggest a sharp boundary makes the transition real, perhaps helping motivate late-movers.

### 5.10 Can the Internet Partition?

In §5.9 we discussed secession and expulsion qualitatively. Threats to secede or sanction have been by countries or groups of countries. If a country were to exert control over their allocated addresses this would result in a country level island or peninsula. We next use our reachability definition of more than 50% to reason quantitatively about control of the IP address space. Our question: Does any country or group have enough addresses to secede and claim to be “the Internet” with a majority of addresses.

To evaluate the power of any country or RIR to control the Internet, Table 8 reports the number of active IPv4 addresses as determined by Internet censuses [38] for each Regional Internet Registry (RIR) and selected countries. Although we define the Internet by active addresses, we cannot currently measure active IPv6 addresses, so we also provide allocated addresses for both v4 and v6 [40, 54]. IPv4 is fully allocated, except for special purpose addresses: loopback (127/8), local and private space (0/8, 10/8, etc. [60]), multicast, and reserved Class E addresses.

We see that no individual RIR or country can secede and take “the Internet”, because none controls the majority of

IPv4 addresses. ARIN has the largest amount with 1673M allocated, that is, 45.2%. Inside ARIN, the United States has the majority of hosts (1617M).

This claim also applies to IPv6, where no RIR or country surpasses a 50% allocation. RIPE (an RIR) is close with 46.7%, and China and the U.S. have high country allocations. With most of IPv6 unallocated, these fractions may change. We note that distribution by region and country is similar for active IPv4 addresses and allocated IPv6 addresses, perhaps because IPv4 allocations are skewed by unused legacy address blocks.

We conclude that no individual country can declare itself “the Internet” without reallocating addresses or colluding with other countries. Suggesting, that the Internet today is an international creation.

## 6 RELATED WORK

A number of works have previously tried to define the Internet [15, 29, 30, 57]. As discussed in §2.1, they distinguish the Internet from other networks of their time, but do not address today’s network disputes and secession threats.

Previous work has looked into the problem of partial outages. RON provides alternate-path routing around failures for a mesh of sites [1]. HUBBLE monitors in real-time reachability problems in which a working physical path exists. LIFEGUARD, proposes a route failure remediation system by generating BGP messages to reroute traffic through a working path [44]. While both solve the problem of partial outages, neither quantifies the amount, duration, or scope of partial outages in the Internet.

Prior work studied partial reachability, showing it is a common transient occurrence during routing convergence [11]. They reproduced partial connectivity with controlled experiments; we study it from Internet-wide vantage points.

Internet scanners have examined bias by location [38], more recently looking for policy-based filtering [77]. We measure policies with our country specific algorithm, and we extend those ideas to defining the Internet.

Outage detection systems have encountered partial outages. Thunderping recognizes the “hosed” state of partial replies as something that occurs, but leaves its study to future work [69]. Trinocular discards partial outages by reporting the target block “up” if any VP can reach it [58]. To the best of our knowledge, prior outage detection systems have not both explained and reported partial outages as part of the Internet, nor studied their extent.

We use the idea of majority to define the Internet in the face of secession. That idea is fundamental in many algorithms for distributed consensus [47, 48, 50], with applications for example to certificate authorities [9].

## 7 CONCLUSIONS

This paper provided a new definition of the Internet to reason about partial connectivity and secession. We developed the algorithm Taitao, to find peninsulas of partial connectivity, and Chiloe, to find islands. We showed that partial connectivity events are more common than simple outages, and used these definitions to clarify outages and the Internet, and to examine issues of sovereignty and evolution.

## ACKNOWLEDGMENTS

The authors would like to thank John Wroclawski, Wes Hardaker, Ramakrishna Padmanabhan, and the Internet Architecture Board for their input on an early version of this paper.

The work is supported in part by the National Science Foundation, CISE Directorate, award CNS-2007106 and NSF-2028279. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

## REFERENCES

- [1] David G. Andersen, Hari Balakrishnan, M. Frans Kaashoek, and Robert Morris. 2001. Resilient Overlay Networks. In *Proceedings of the Symposium on Operating Systems Principles*. ACM, Chateau Lake Louise, Alberta, Canada, 131–145. <http://www-cse.ucsd.edu/sosp01/papers/andersen.pdf>
- [2] Anonymous. 2012. The collateral damage of Internet censorship by DNS injection. *ACM Computer Communication Review* 42, 3 (July 2012), 21–27. <https://doi.org/10.1145/2317307.2317311>
- [3] Anonymous. 2014. Towards a Comprehensive Picture of the Great Firewall’s DNS Censorship. In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet*. USENIX, San Diego, CA, USA, 7 pages. <https://www.usenix.org/system/files/conference/foci14/foci14-anonymous.pdf>
- [4] ANT Project. 2022. ANT IPv4 Island and Peninsula Data. [https://ant.isi.edu/datasets/ipv4\\_partial/](https://ant.isi.edu/datasets/ipv4_partial/). [https://ant.isi.edu/datasets/ipv4\\_partial/](https://ant.isi.edu/datasets/ipv4_partial/)
- [5] Cathy Aronson. 2015. To Squat Or Not To Squat? blog <https://teamarin.net/2015/11/23/to-squat-or-not-to-squat/>. <https://teamarin.net/2015/11/23/to-squat-or-not-to-squat/>
- [6] ArsTechnica. 2010. Peering problems: digging into the Comcast/Level 3 grudge match. <https://arstechnica.com/tech-policy/2010/12/comcastlevel3/>.
- [7] Guillermo Baltra and John Heidemann. 2020. Improving Coverage of Internet Outage Detection in Sparse Blocks. In *Proceedings of the Passive and Active Measurement Workshop*. Springer, Eugene, Oregon, USA. <https://www.isi.edu/%7Ejohnh/PAPERS/Baltra20a.html>
- [8] Genevieve Bartlett, John Heidemann, and Christos Papadopoulos. 2007. Understanding Passive and Active Service Discovery. In *Proceedings of the ACM Internet Measurement Conference*. ACM, San Diego, California, USA, 57–70. <https://doi.org/10.1145/1298306.1298314>
- [9] Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. 2018. Bamboozling certificate authorities with BGP. In *27th USENIX Security Symposium*. USENIX, Baltimore, Maryland, USA, 833–849.
- [10] Scott Burleigh, Vinton Cerf, Robert Durst, Kevin Fall, Adrian Hooke, Keith Scott, and Howard Weiss. 2003. The InterPlaNetary Internet: a communications infrastructure for Mars exploration. *Acta astronautica*

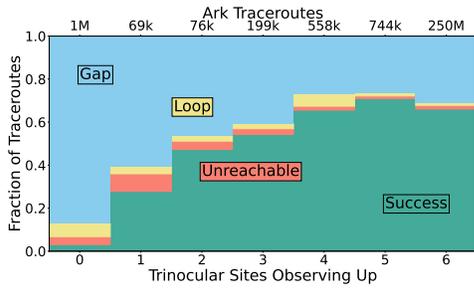
- 53, 4-10 (2003), 365–373.
- [11] Randy Bush, Olaf Maennel, Matthew Roughan, and Steve Uhlig. 2009. Internet optometry: assessing the broken glasses in Internet reachability. In *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement* (Chicago, Illinois, USA). ACM, 242–253. <http://www.maennel.net/2009/imc099-bush.pdf>
- [12] CAIDA. 2007. Archipelago (Ark) Measurement Infrastructure. website <https://www.caida.org/projects/ark/>. <https://www.caida.org/projects/ark/>
- [13] CAIDA. 2017. 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](https://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml).
- [14] CAIDA. 2020. 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](https://www.caida.org/data/active/ipv4_routed_24_topology_dataset.xml).
- [15] Vint Cerf and Robert Kahn. 1974. A Protocol for Packet Network Interconnection. *IEEE Transactions on Communications COM-22*, 5 (May 1974), 637–648. <http://sysnet.ucsd.edu/classes/cse222/wi03/papers/cerf-tcp-toc74.pdf>
- [16] David D. Clark. 1988. The Design Philosophy of the DARPA Internet Protocols. In *Proceedings of the 1988 Symposium on Communications Architectures and Protocols* (johnh: folder: networking). ACM, 106–114.
- [17] CNBC. 2019. Russia just brought in a law to try to disconnect its Internet from the rest of the world. <https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html>.
- [18] Cogent. 2021. Looking Glass. <https://cogentco.com/en/looking-glass>.
- [19] James Cowie. 2011. Egypt Leaves the Internet. Resenys Blog <http://www.renysys.com/blog/2011/01/egypt-leaves-the-internet.shtml> <http://www.renysys.com/blog/2011/01/egypt-leaves-the-internet.shtml>
- [20] RBC daily. 2021. Russia, tested the Runet when disconnected from the Global Network. website [https://www.rbc.ru/technology\\_and\\_media/21/07/2021/60f8134c9a79476f5de1d739](https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739). [https://www.rbc.ru/technology\\_and\\_media/21/07/2021/60f8134c9a79476f5de1d739](https://www.rbc.ru/technology_and_media/21/07/2021/60f8134c9a79476f5de1d739)
- [21] Alberto Dainotti, Claudio Squarcella, Emile Aben, Marco Chiesa, Kimberly C. Claffy, Michele Russo, and Antonio Pescapé. 2011. Analysis of Country-wide Internet Outages Caused by Censorship. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Berlin, Germany, 1–18. <https://doi.org/10.1145/2068816.2068818>
- [22] Dhaka Tribune Desk. 2018. Internet services to be suspended across the country. *Dhaka Tribune* (Feb. 11 2018). <http://www.dhakatribune.com/regulation/2018/02/11/internet-services-suspended-throughout-country/>
- [23] Amogh Dhamdhere, David D. Clark, Alexander Gamero-Garrido, Matthew Luckie, Ricky K. P. Mok, Gautam Akiwate, Kabir Gogia, Vaibhav Bajpai, Alex C. Snoeren, and kc claffy. 2018. Inferring Persistent Interdomain Congestion. In *Proceedings of the ACM SIGCOMM Conference*. ACM, Budapest, Hungary, 1–15. <https://doi.org/10.1145/3230543.3230549>
- [24] DINRG. 2021. Decentralized Internet Infrastructure Research Group. <https://irtf.org/dinrg>.
- [25] Peter K. Dunn. 2021. Scientific Research Methods. <https://bookdown.org/pkaldunn/Book/>.
- [26] Zakir Durumeric, Michael Bailey, and J Alex Halderman. 2014. An Internet-wide view of Internet-wide scanning. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. USENIX, San Diego, California, USA, 65–78. <https://jhalderm.com/pub/papers/scanning-sec14.pdf>
- [27] Economist Editors. 2018. Why some countries are turning off the internet on exam days. *The Economist* (July 5 2018). <https://www.economist.com/middle-east-and-africa/2018/07/05/why-some-countries-are-turning-off-the-internet-on-exam-days> (Appeared in the Middle East and Africa print edition).
- [28] Hurricane Electric. 2021. Looking Glass. <http://lg.he.net/>.
- [29] Engadget. 2020. China, Huawei propose internet protocol with a built-in killswitch. <https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html>.
- [30] Federal Networking Council (FNC). 1995. Definition of “Internet”. [https://www.nitrd.gov/historical/fnc/internet\\_res.pdf](https://www.nitrd.gov/historical/fnc/internet_res.pdf).
- [31] HE forums. 2017. Cloudflare Blocked on Free Tunnels now? <https://forums.he.net/index.php?topic=3805.0>.
- [32] V. Fuller, E. Lear, and D. Meyer. 2008. Reclassifying 240/4 as usable unicast address space. (March 2008). <https://datatracker.ietf.org/doc/html/draft-fuller-240space-02> Work in progress (Internet draft draft-fuller-240space-02.txt).
- [33] Samuel Gibbs. 1996. Iraq shuts down the Internet to stop pupils cheating in exams. *The Guardian* (18 May 1996). <https://www.theguardian.com/technology/2016/may/18/iraq-shuts-down-internet-to-stop-pupils-cheating-in-exams>
- [34] Google. 2021. Google IPv6 Statistics. <https://www.google.com/intl/en/ipv6/statistics.html>.
- [35] Albert Greenberg, James R. Hamilton, Navendu Jain, Srikanth Kandula, Changhoon Kim, Parantap Lahiri, David A. Maltz, and Parveen Pat. 2009. VL2: A Scalable and Flexible Data Center Network. In *Proceedings of the ACM SIGCOMM Conference* (johnh: pafile). ACM, Barcelona, Spain, 51–62. <http://ccr.sigcomm.org/online/files/p51.pdf>
- [36] Andreas Guillot, Romain Fontugne, Philipp Winter, Pascal Merindol, Alistair King, Alberto Dainotti, and Cristel Pelsser. 2019. Chocolate: Outage Detection for Internet Background Radiation. In *Proceedings of the IFIP International Workshop on Traffic Monitoring and Analysis*. IFIP, Paris, France, 8 pages. <https://clarinet.u-strasbg.fr/~pelsser/publications/Guillot-chocolate-TMA2019.pdf>
- [37] Hang Guo and John Heidemann. 2018. Detecting ICMP Rate Limiting in the Internet. In *Proceedings of the Passive and Active Measurement Workshop* (johnh: pafile). Springer, Berlin, Germany, to appear. <https://www.isi.edu/%7Ejohnh/PAPERS/Guo18a.html>
- [38] John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett, and Joseph Bannister. 2008. Census and Survey of the Visible Internet. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Vouliagmeni, Greece, 169–182. <https://doi.org/10.1145/1452520.1452542>
- [39] Jon Henley. 2018. Algeria blocks internet to prevent students cheating during exams. *The Guardian* (22 June 2018). <https://www.theguardian.com/world/2018/jun/21/algeria-shuts-internet-prevent-cheating-school-exams>
- [40] IANA. 2021. IPv6 RIR Allocation Data. <https://www.iana.org/numbers/allocations/>.
- [41] Internet Architecture Board. 2000. *IAB Technical Comment on the Unique DNS Root*. RFC 2826. Internet Request For Comments. <https://www.rfc-editor.org/rfc/rfc2826>
- [42] IPNSIG. 2020. InterPlanetary Networking Special Interest Group. <http://ipnsig.org/>.
- [43] Ethan Katz-Bassett, Harsha V Madhyastha, John P John, Arvind Krishnamurthy, David Wetherall, and Thomas E Anderson. 2008. Studying Black Holes in the Internet with Hubble. In *Proceedings of the USENIX Conference on Networked Systems Design and Implementation*. ACM, San Francisco, CA, 247–262.
- [44] Ethan Katz-Bassett, Colin Scott, David R. Choffnes, Ítalo Cunha, Vytautas Valancius, Nick Feamster, Harsha V. Madhyastha, Tom Anderson, and Arvind Krishnamurthy. 2012. LIFE GUARD: Practical Repair of Persistent Route Failures. In *Proceedings of the ACM SIGCOMM Conference*. ACM, Helsinki, Finland, 395–406. <https://doi.org/10.1145/2377677.2377756>
- [45] DataCenter Knowledge. 2009. Peering Disputes Migrate to IPv6. <https://www.datacenterknowledge.com/archives/2009/10/22/>

- peering-disputes-migrate-to-ipv6.
- [46] Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian. 2010. Internet Inter-Domain Traffic. In *Proceedings of the ACM SIGCOMM Conference*. ACM, New Delhi, India, 75–86. <https://doi.org/10.1145/1851182.1851194>
- [47] Leslie Lamport. 1998. The Part-Time Parliament. *ACM Transactions on Computer Systems* 16, 2 (May 1998), 133–169. <https://doi.org/10.1145/279227.279229>
- [48] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems* 4, 3 (July 1982), 382–401.
- [49] D. Meyer. 2018. University of Oregon Routeviews. <http://www.routeviews.org>.
- [50] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. Released publicly <http://bitcoin.org/bitcoin.pdf>
- [51] RIPE NCC. 2021q3. 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]/).
- [52] RIPE NCC. 2021q3. 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]/).
- [53] BBC News. 2019. Russia internet: Law introducing new controls comes into force. website <https://www.bbc.com/news/world-europe-50259597>
- [54] NRO. 2021. IPv4 Address Space Registry. <https://www.nro.net/about/rirs/statistics/>.
- [55] Ramakrishna Padmanabhan, Amogh Dhamdhere, Emile Aben, kc claffy, and Neil Spring. 2016. Reasons Dynamic Addresses Change. In *Proceedings of the ACM Internet Measurement Conference* (johnh: pafille). ACM, Santa Monica, CA, USA, 183–198. <https://doi.org/10.1145/2987443.2987461>
- [56] C. Partridge, T. Mendez, and W. Milliken. 1993. *Host Anycasting Service*. RFC 1546. Internet Request For Comments. <https://www.rfc-editor.org/rfc/rfc1546.txt>
- [57] Jonathan B. Postel. 1980. Internetwork Protocol Approaches. *IEEE Trans. Comput.* 28, 4 (April 1980), 604–611. <https://doi.org/10.1109/TCOM.1980.1094705>
- [58] Lin Quan, John Heidemann, and Yuri Pradkin. 2013. Trinocular: Understanding Internet Reliability Through Adaptive Probing. In *Proceedings of the ACM SIGCOMM Conference*. ACM, Hong Kong, China, 255–266. <https://doi.org/10.1145/2486001.2486017>
- [59] Dan Rayburn. 2016. Google Blocking IPv6 Adoption With Cogent, Impacting Transit Customers. <https://seekingalpha.com/article/3948876-google-blocking-ipv6-adoption-cogent-impacting-transit-customers>.
- [60] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. 1996. *Address Allocation for Private Internets*. RFC 1918. Internet Request For Comments. <ftp://ftp.rfc-editor.org/in-notes/rfc1918.txt>
- [61] Reuters. 2021. 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/>
- [62] Reuters. 2022. website <https://www.reuters.com/technology/us-firm-cogent-cutting-internet-service-russia-2022-03-04/>
- [63] Philipp Richter, Ramakrishna Padmanabhan, Neil Spring, Arthur Berger, and David Clark. 2018. Advancing the Art of Internet Edge Outage Detection. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Boston, Massachusetts, USA, 350–363. <https://doi.org/10.1145/3278532.3278563>
- [64] Philipp Richter, Florian Wohlfart, Narseo Vallina-Rodriguez, Mark Allman, Randy Bush, Anja Feldmann, Christian Kreibich, Nicholas Weaver, and Vern Paxson. 2016. A Multi-perspective Analysis of Carrier-Grade NAT Deployment. In *Proceedings of the ACM Internet Measurement Conference* (johnh: pafille). ACM, Santa Monica, CA, USA. <https://doi.org/10.1145/2987443.2987474>
- [65] RIPE NCC. 2020. DNSMON. <https://atlas.ripe.net/dnsmon>.
- [66] RIPE NCC Staff. 2015. RIPE Atlas: A Global Internet Measurement Network. *The Internet Protocol Journal* 18, 3 (Sept. 2015), 2–26.
- [67] Sen. John D. Rockefeller. 2009. Cybersecurity Act of 2010. <https://www.congress.gov/bill/111th-congress/senate-bill/773>.
- [68] J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy. 2003. *STUN—Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)*. RFC 3489. Internet Request For Comments. <ftp://ftp.rfc-editor.org/in-notes/rfc3489.txt>
- [69] Aaron Schulman and Neil Spring. 2011. Pingin’ in the Rain. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Berlin, Germany, 19–25. <https://doi.org/10.1145/2068816.2068819>
- [70] Anant Shah, Romain Fontugne, Emile Aben, Cristel Pelsser, and Randy Bush. 2017. Disco: Fast, Good, and Cheap Outage Detection. In *Proceedings of the IEEE International Conference on Traffic Monitoring and Analysis*. Springer, Dublin, Ireland, 1–9. <https://doi.org/10.23919/TMA.2017.8002902>
- [71] Xiao Song and John Heidemann. 2021. *Measuring the Internet during Covid-19 to Evaluate Work-from-Home*. Technical Report arXiv:2102.07433v2 [cs.NI]. USC/ISI. <https://www.isi.edu/%7ejohnh/PAPERS/Song21a.html>
- [72] Craig Timberg and Paul Sonne. 2021. Minutes before Trump left office, millions of the Pentagon’s dormant IP addresses sprang to life. *The Washington Post* (Apr. 24 2021). <https://www.washingtonpost.com/technology/2021/04/24/pentagon-internet-address-mystery/>
- [73] Paul F. Tsuchiya and Tony Eng. 1993. Extending the IP Internet Through Address Reuse. *ACM Computer Communication Review* 23, 1 (Jan. 1993), 16–33. <http://www.cs.cornell.edu/People/francis/tsuchiya93extending.pdf>
- [74] European Union. 2021. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [75] USC/ISI ANT project. 2017. <https://ant.isi.edu/datasets/all.html>. Accessed: 2019-01-08.
- [76] USC/LANDER Project. 2014. Internet Outage Measurements. listed on web page <https://ant.isi.edu/datasets/outage/>.
- [77] Gerry Wan, Liz Izhikevich, David Adrian, Katsunari Yoshioka, Ralph Holz, Christian Rossow, and Zakir Durumeric. 2020. On the Origin of Scanning: The Impact of Location on Internet-Wide Scans. In *Proceedings of the ACM Internet Measurement Conference*. ACM, Pittsburgh, PA, USA, 662–679. <https://doi.org/10.1145/3419394.3424214>
- [78] Samuel Woodhams and Simon Migliano. 2021. The Global Cost of Internet Shutdowns in 2020. <https://www.top10vpn.com/cost-of-internet-shutdowns/>.

## A RESEARCH ETHICS

Our work poses no ethical concerns for several reasons.

First, we collect no additional data, but instead reanalyze data from several existing sources listed in §B. Our work therefore poses no additional risk in data collection.



**Figure 6: Ark traceroutes sent to targets under partial outages (2017-10-10 to -31). Dataset A30.**

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

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

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

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

## B DATA SOURCES USED HERE

Table 9 provides a full list of datasets used in this paper and where they may be obtained.

## C OUTAGES REVISITED

### C.1 Observed Outage and External Data

To evaluate outage classification with conflicting information, we consider Trinocular reports and compare to external information in traceroutes from CAIDA Ark.

Figure 6 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 5 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.

We observe that 5 sites show the same results as all 6, so single-VP failures likely represent problems local to that VP. This suggests that all-but-one is a good algorithm to determine 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 3.

### C.2 Are the Sites Independent?

Our evaluation assumes VPs do not share common network paths. Two VPs in the same location would share the same local outages, but those in different physical locations will often use different network paths, particularly with a “flatter” Internet graph [46]. We next quantify this similarity to validate our assumption.

We next measure similarity of observations between pairs of VPs. We examine only cases where one of the pair disagrees with some other VP, since when all agree, we have no new information. If the pair agrees with each other, but not with the majority, the pair shows similarity. If they disagree with each other, they are dissimilar. We quantify similarity  $S_P$  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 on the network having state  $s$  of up (1) or down (0) and disagrees with the others, and for  $D_*$ , the pair disagrees with each other.  $S_P$  ranges from 1, where the pair always agrees, to 0, where they always disagree.

Table 10(a) shows similarity values for each pair of the 6 Trinocular VPs. (We show only half of the symmetric matrix.)

Dataset Name	Source	Start Date	Duration	Where Used
internet_outage_adaptive_a28w-20170403	Trinocular [75]	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§2.3.2, §D
internet_outage_adaptive_a28c-20170403	Trinocular	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§D
internet_outage_adaptive_a28j-20170403	Trinocular	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§D
internet_outage_adaptive_a28g-20170403	Trinocular	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§D
internet_outage_adaptive_a28e-20170403	Trinocular	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§2.3.2, §D
internet_outage_adaptive_a28n-20170403	Trinocular	2017-04-03	90 days	
Polish peninsula subset		2017-06-03	12 hours	§2.3.2, §D
internet_outage_adaptive_a28all-20170403	Trinocular	2017-04-03	89 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a29all-20170702	Trinocular	2017-07-02	94 days	§2.3.2, §4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a30w-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§2.3.3, §D
internet_outage_adaptive_a30c-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§D
internet_outage_adaptive_a30j-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§D
internet_outage_adaptive_a30g-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§D
internet_outage_adaptive_a30e-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§2.3.3, §D
internet_outage_adaptive_a30n-20171006	Trinocular	2017-10-06	85 days	
Site E Island		2017-10-23	36 hours	§2.3.3, §D
internet_outage_adaptive_a30all-20171006	Trinocular	2017-10-06	85 days	§4.3, §5.6, §5.7, §C.2, §E.3
Oct. Nov. subset		2017-10-06	40 days	§4.2, §5.2, §5.3
Oct. subset		2017-10-10	21 days	§4.1, §C.1
internet_outage_adaptive_a31all-20180101	Trinocular	2018-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a32all-20180401	Trinocular	2018-04-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a33all-20180701	Trinocular	2018-07-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a34all-20181001	Trinocular	2018-10-01	90 days	§4.3, §5.6, §5.7, §F.1, §E.3
internet_outage_adaptive_a35all-20190101	Trinocular	2019-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a36all-20190401	Trinocular	2019-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a37all-20190701	Trinocular	2019-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a38all-20191001	Trinocular	2019-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a39all-20200101	Trinocular	2020-01-01	90 days	§4.3, §5.6, §5.7, §E.3
internet_outage_adaptive_a41all-20200701	Trinocular	2020-07-01	90 days	§5.4
prefix-probing	Ark [12]			
Oct. 2017 subset		2017-10-10	21 days	§4.1, §C.1
2020q3 subset		2020-07-01	90 days	§5.4
probe-data	Ark			
Oct 2017 subset		2017-10-10	21 days	§4.1, §C.1
2020q3 subset		2020-07-01	90 days	§5.4
routeviews.org/bgpdata	Routeviews [49]	2017-10-06	40 days	§4.2, §D
Atlas Recurring Root Pings (id: 1001 to 1016)	Atlas [51]	2021-07-01	90 days	§5.1, §5.7
nro-extended-stats	NRO [40, 54]	1984	41 years	§5.10

**Table 9: All datasets used in this paper.**

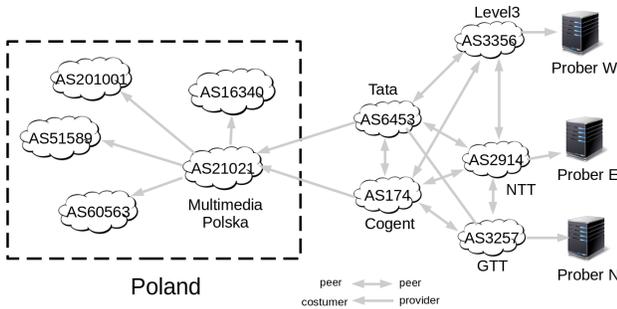
No two sites have a similarity more than 0.14, and most pairs are under 0.08. This result shows that no two sites are particularly correlated.

## D VALIDATION OF THE POLISH PENINSULA

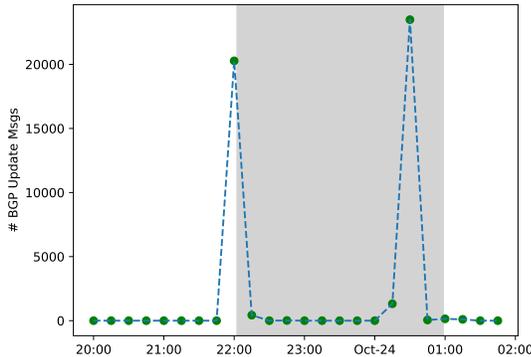
On 2017-10-23, for a period of 3 hours starting at 22:02Z, five Polish ASes had 1716 blocks that were unreachable from five

	C	J	G	E	N
W	0.017	0.031	0.019	0.035	0.020
C		0.077	0.143	0.067	0.049
J			0.044	0.036	0.046
G				0.050	0.100
E					0.058

**Table 10: Similarities between sites relative to all six. Dataset: A30, 2017q4.**



**Figure 7: AS level topology during the Polish peninsula.**

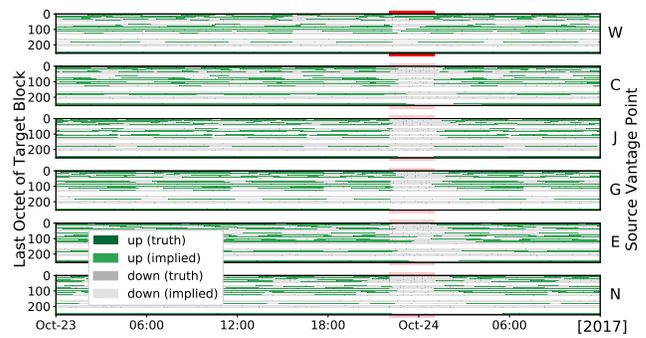


**Figure 8: BGP update messages sent for affected Polish blocks starting 2017-10-23T20:00Z. Data source: RouteViews.**

VPs while the same blocks remained reachable from a sixth VP.

Figure 7 shows the AS-level relationships at the time of the peninsula. Multimedia Polska (AS21021, or MP) provides service to the other 4 ISPs. MP has two Tier-1 providers: Cogent (AS174) and Tata (AS6453). Before the peninsula, our VPs see MP through Cogent.

At event start, we observe many BGP updates (20,275) announcing and withdrawing routes to the affected blocks (see Figure 8). These updates correspond to Tata announcing MP's



**Figure 9: A block (80.245.176.0/24) showing a 3-hour peninsula accessible only from VP W (top bar) and not from the other five VPs. Dataset: A30.**

prefixes. Perhaps MP changed its peering to prefer Tata over Cogent, or the MP-Cogent link failed.

Initially, traffic from most VPs continued through Cogent and was lost; it did not shift to Tata. One VP (W) could reach MP through Tata for the entire event, proving MP was connected. After 3 hours, we see another burst of BGP updates (23,487 this time), making MP reachable again from all VPs.

In Figure 9 we provide data from our 6 external VPs, where W is uniquely capable of reaching the target block, thus living in the same peninsula.

We further verify this event by looking at traceroutes. During the event we see 94 unique Ark VPs attempted 345 traceroutes to the affected blocks. Of the 94 VPs, 21 VPs (22%) have their last responsive traceroute hop in the same AS as the target address, and 68 probes (73%) stopped before reaching that AS. Table 11 shows traceroute data from a single CAIDA Ark VP before and during the peninsula described in §2.3.3 and Figure 2. This data confirms the block was reachable from some locations and not others. During the event, this trace breaks at the last hop within the source AS.

## E ADDITIONAL DETAILS ABOUT ISLANDS

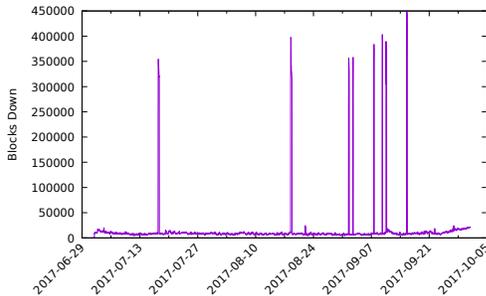
### E.1 Country-sized Islands

In §2.3.2 we defined islands and gave a sample. We also have seen country-sized islands.

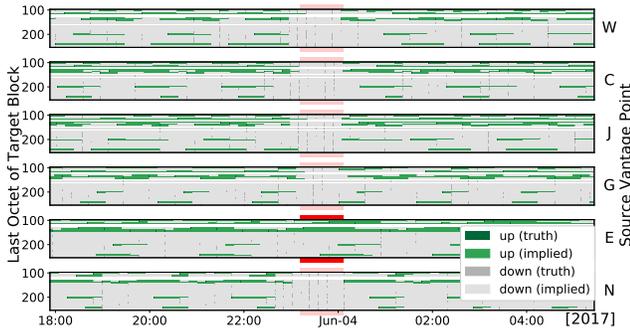
In 2017q3 we observed 8 events when it appears that most or all of China stopped responding to external pings. Figure 10 shows the number of /24 blocks that were down over time, each spike more than 200k /24s, between two to eight hours long. We found no problem reports on network operator mailing lists, so we believe these outages were ICMP-specific and likely did not affect web traffic. In addition, we assume the millions of computers inside China continued to

src block	dst block	time	traces
c85eb700	50f5b000	1508630032	q, 148.245.170.161, 189.209.17.197, 189.209.17.197, 38.104.245.9, 154.24.19.41, 154.54.47.33, 154.54.28.69, 154.54.7.157, 154.54.40.105, 154.54.40.61, 154.54.43.17, 154.54.44.161, 154.54.77.245, 154.54.38.206, 154.54.60.254, 154.54.59.38, 149.6.71.162, 89.228.6.33, 89.228.2.32, 176.221.98.194
c85eb700	50f5b000	1508802877	q, 148.245.170.161, 200.38.245.45, 148.240.221.29

**Table 11: Traces from the same Ark VPs (mty-mx) to the same destination before and during the event block**



**Figure 10: Number of blocks down in the whole responsive Internet. Dataset: A29, 2017q3.**



**Figure 11: A block showing a 1-hour island for this block and VP E, while other five VPs cannot reach it.**

operate. We consider these cases examples of China becoming an *ICMP-island*.

### E.2 Validation of the Sample Island

In §2.3.2 we reported an island affecting a /24 block where VP E lives. During the time of the event, E was able to successfully probe addresses within the same block, however, unable to reach external addresses. This event started at 2017-06-03t23:06Z, and can be observed in Figure 12.

Furthermore, no other VP was able to reach the affected block for the time of the island as shown in Figure 11.

### E.3 Longitudinal View Of Islands

We first consider three years of Trinocular data (described in §3.1), from 2017-04-01 to 2020-04-01. Figure 12 shows the fraction of the Internet that is reachable as a dotted line at the 50% threshold that Chiloe uses to detect an island (§3.4). We run Chiloe across each VP for this period.

## F ADDITIONAL RESULTS

Our paper body uses Trinocular measurements for 2017q4 because this time period had six active VPs, allowing us to make strong statements about how multiple perspectives help. In this section, we verify our results using newer datasets to confirm our prior results still hold. They do—we find quantitatively similar results between 2017 and 2020.

### F.1 Additional Confirmation of the Number of Peninsulas

Similarly, as in §5.1, we quantify how big the problem of peninsulas is, this time using Trinocular 2018q4 data.

In Figure 13 we confirm, that with more VPs more peninsulas are discovered, providing a better view of the Internet’s overall state.

*Outages (left) converge after 3 sites*, as shown by the fitted curve and decreasing variance. Peninsulas and all-up converge more slowly.

At six VPs, here we find an even higher difference between all down and disagreements. Confirming that peninsulas are a more pervasive problem than outages.

### F.2 Additional Confirmation of Peninsula Duration

In §5.2 we characterize peninsula duration for 2017q4, to determine peninsula root causes. To confirm our results, we repeat the analysis, but with 2020q3 data.

As Figure 14a shows, similarly, as in our 2017q4 results, we see that there are many very brief peninsulas (from 20 to 60 minutes). These results suggest that while the Internet is robust, there are many small connectivity glitches.

Events shorter than two rounds (22 minutes), may represent BGP transients or failures due to random packet loss.



we use 2017q4 data. Here we use 2020q3 to confirm our results.

Figure 14b shows the peninsulas per prefix fraction, and Figure 14c. Similarly, we find that while small prefix fraction

peninsulas are more in numbers, most of the peninsula time is spent in peninsulas covering the whole prefix. This result is consistent with long lived peninsulas being caused by policy choices.