RAN: Routing Around Nation-States

Anne Edmundson, Roya Ensafi, Nick Feamster, Jennifer Rexford
Princeton University

Abstract

Many countries now engage in interference, degradation, blocking, or surveillance of Internet traffic. In response, individuals, organizations, and even entire countries are taking steps to control the geographic regions that their traffic traverses. For example, some countries are building local Internet Exchange Points (IXPs) to prevent domestic traffic from detouring through other countries. Unfortunately, our measurements reveal that many such ongoing efforts are futile, for two reasons: local content is often hosted in foreign countries, and networks within a country often fail to peer with one another. Yet, our work offers hope: we also find that routing traffic through strategically placed relay nodes can reduce transnational routing detours, in the best case, from 85% of studied paths to 38% of studied paths; using DNS open resolvers to help clients discover and use different replicas of the same service can also reduce transnational detours by about 4%. Based on these findings, we design and implement RAN, a lightweight system that automatically routes a client's web traffic around specified countries with no modifications to client software (and in many cases with little performance overhead). Anyone can use RAN today; we have deployed long-running RAN Web proxy relays around the world, released the source code, and provided instructions for configuring a client to use the system.

1 Introduction

When Internet traffic enters a country, it becomes subject to that country's laws. As a result, users have more need than ever to determine—and control—which countries their traffic is traversing. An increasing number of countries have passed laws that facilitate mass surveillance of their networks [25, 33, 36, 41], and governments and citizens are increasingly motivated to divert their Internet traffic from countries that perform surveillance (notably, the United States [18, 19, 50]).

Many countries—notably, Brazil—are taking impressive measures to reduce the likelihood that Internet traffic transits the United States [10–12, 15, 31] including building a 3,500-mile long fiber-optic cable from Fortaleza to Portugal (with no use of American vendors); pressing companies such as Google, Facebook, and Twitter (among others) to store data locally; and mandating the deployment of a state-developed email system (Expresso) throughout the federal government (instead of what was originally used, Microsoft Outlook) [9, 13]. Brazil is also building Internet Exchange Points (IXPs) [8], now has the largest national ecosystem of public IXPs in the world [16], and the number of internationally connected Autonomous Systems (ASes) continues to grow [14]. Brazil is not alone: IXPs are proliferating in eastern Europe, Africa, and other regions, in part out of a desire to "keep local traffic local". Building IXPs alone, of course, cannot guarantee that Internet traffic for some service does not enter or transit a particular country: Internet protocols have no notion of national borders, and interdomain paths depend in large part on existing interconnection business relationships (or lack thereof).

Although end-to-end encryption stymies surveillance by concealing URLs and content, it does not by itself protect all sensitive information from prying eyes. First, many websites do not fully support encrypted browsing by default; a recent study showed that more than 85% of the most popular health, news, and shopping sites do not encrypt by default [59]; migrating a website to HTTPS is challenging, and doing so requires all third-party domains on the site (including advertisers) to use HTTPS. Second, even encrypted traffic may still reveal a lot about user behavior: the presence of any communication at all may be revealing, and website fingerprinting can reveal information about content merely based on the size, content, and location of third-party resources that a client loads. DNS traffic is also quite revealing and is essentially never encrypted [59]. Third, ISPs often terminate TLS connections, conducting man-in-the-middle attacks on encrypted traffic for network management purposes [28]. Circumventing surveillance thus requires not only encryption, but also mechanisms for controlling where traffic goes in the first place.

In this paper, we study two questions: (1) Which countries do *default* Internet routing paths traverse?; (2) What methods can help increase hosting and path diversity to help governments and citizens better control transnational Internet paths? In contrast to previous work [35], which simulates Internet paths, we *actively measure* and analyze the paths originating in five different countries: Brazil, Netherlands, Kenya, India, and the United States. We study these countries for different reasons, including their efforts made to avoid certain countries, efforts in building out IXPs, and their low cost of hosting domains. Our work studies the router-level forwarding path, which differs from all other work in this area, which has focused on analyzing Border Gateway Protocol (BGP) routes [35,52]. Although BGP routing can offer useful information about paths, it does not necessarily reflect the path that traffic actually takes, and it only provides AS-level granularity, which is often too coarse to make strong statements about which countries that traffic is traversing. In contrast, we measure traffic routes from RIPE Atlas probes in five countries to the Alexa Top 100 domains for each country; we directly measure the paths not only to the websites corresponding to themselves, but also to the sites hosting any third-party content on each of these sites.

Determining which countries a client's traffic traverses is challenging, for several reasons. First, performing direct measurements is more costly than passive analysis of BGP routing tables; RIPE Atlas, in particular, limits the rate at which one can perform measurements. As a result, we had to be strategic about the origins and destinations that we selected for our study. As we explain in Section 3, we study five geographically diverse countries, focusing on countries in each region that are making active attempts to thwart transnational Internet paths. Second, IP geolocation—the process of determining the geographic location of an IP address—is notoriously challenging, particularly for IP addresses that represent Internet infrastructure, rather than end-hosts. We cope with this inaccuracy by making conservative estimates of the extent of routing detours, and by recognizing that our goal is not to pinpoint a precise location for an IP address as much as to achieve accurate reports of *significant* off-path detours to certain countries or regions. (Section 4 explains our method in more detail; we also explicitly highlight ambiguities in our results.) Finally, the asymmetry of Internet paths can also make it difficult to analyze the countries that traffic traverses on the reverse path from server to client; our study finds that country-level paths are often asymmetric, and, as such, our findings represent a lower bound on transnational routing detours.

The first part of our study (Section 4) characterizes the current state of transnational Internet routing detours. We first explore hosting diversity and find that only about half of the Alexa Top 100 domains in the five countries studied are hosted in more than one country, and many times that country is a surveillance state that clients may want to avoid. Second, even if hosting diversity can be improved, routing can still force traffic through a small collection of countries (often surveillance states). Despite strong efforts made by some countries to ensure their traffic does not transit unfavorable countries [10–12, 15, 31], their traffic still traverses surveillance states. Over 50% of the top domains in Brazil and India are hosted in the United States, and over 50% of the paths from the Netherlands to the top domains transit the United States. About half of Kenyan paths to the top domains traverse the United States and Great Britain (but the same half does not traverse both countries). Much of this phenomenon is due to "tromboning", whereby an Internet path starts and ends in a country, yet transits an intermediate country; for example, about 13% of the paths that we explored from Brazil tromboned through the United States. Infrastructure building alone is not enough: ISPs in respective regions need better encouragements to interconnect with one another to ensure that local traffic stays local.

The second part of our work (Section 5) explores potential mechanisms for avoiding certain countries, and the potential effectiveness of these techniques. We explore two techniques: using the open DNS resolver infrastructure and using overlay network relays. We find that both of these techniques can be effective for clients in certain countries, yet the effectiveness of each technique also depends on the county. For example, Brazilian clients could completely avoid Spain, Italy, France, Great Britain, Argentina, and Ireland (among others), even though the default paths to many popular Brazilian sites traverse these countries. We also find that some of the most prominent surveillance states are also some of the least avoidable countries. For example, many countries depend on ISPs in the United States, a known surveillance state, for connectivity to popular sites and content. Additionally, overlay network relays can keep local traffic local: by using relays in the client's country, fewer paths trombone out of the client's country.

The third part of our work (Section 7) uses the most effective country avoidance technique — overlay nework relays — in a lightweight system, RAN, that allows a client to access web content without traversing an undesirable country. The system uses a series of overlay network relays to automatically routes a client's traffic around a specified country. We design and implement RAN for country avoidance, usability, and scalability. Our evaluation shows that our system is effective for avoiding different countries, while having negligible performance overhead — sometimes having better performance than when no country avoidance system is used.

2 Related Work

Nation-state routing analysis. Recently, Shah and Papadopoulos measured international BGP detours (paths that originate in one country, cross international borders, and then return to the original country) [52]. Using BGP routing tables, they found 2 million detours in each month of their study (out of 7 billion total paths), and they then characterized the detours based on detour dynamics and persistence. Our work differs by actively measuring traceroutes (actual paths), as opposed to analyzing BGP routes. This difference is fundamental as BGP provides the AS path announced in BGP update messages, which is not necessarily the same as the actual path of data packets. Obar and Clement analyzed traceroutes that started and ended in Canada, but "boomeranged" through the United States ("boomerang" is another term for tromboning), and argued that this is a violation of Canadian network sovereignty [43]. Most closely related to our work, Karlin et al. developed a framework for country-level routing analysis to study how much influence each country has over interdomain routing [35]. This work measures the centrality of a country to routing and uses AS-path inference to measure and quantify country centrality, whereas our work uses active measurements and measures avoidability of a given country.

Mapping national Internet topologies. In 2011, Roberts et al. described a method for mapping national networks of ASes, identifying ASes that act as points of control in the national network, and measuring the complexity of the national network [49]. There have also been a number of studies that measured and classified the network within a country. Wahlisch et al. measured and classified the ASes on the German Internet [56, 57], Zhou et al. measured the complete Chinese Internet topology at the AS level [60], and Bischof et al. characterized the current state of Cuba's connectivity with the rest of the world [7]. Interconnectivity has also been studied at the continent level; Gupta et al. first looked at ISP interconnectivity within Africa [29], and it was studied later by Fanou et al. [23].

Circumvention and Routing Systems. There has been research into circumvention systems, particularly for censorship circumvention, that is related this work, but not sufficient for surveillance circumvention. Tor is an anonymity system that uses three relays and layered encryption to allow users to communicate anonymously [20]. VPNGate is a public VPN relay system aimed at circumventing national firewalls [42]. Unfortunately, VPNGate does not allow a client to choose any available VPN, which makes surveillance avoidance harder. Another system, Alibi Routing, is a peer-to-peer system that uses round trip times to prove that that a client's packets did not traverse a forbidden country or region [38]; our work differs by measuring which countries a client's packets would (and do) traverse. Our work then uses active measurements to determine the best path for a client wishing to connect to a server. RON, Resilient Overlay Networks, is an overlay network that routes around failures, whereas our overlay network routes around countries [1].

3 State of Surveillance and Interference

We focused our study on five different countries, and for each, we actively measured and analyzed traffic that originated there. These five countries were chosen for specific reasons and we present them here. We also discuss countries that currently conduct interference, degradation, blocking, and/or surveillance; this exploration is not exhaustive, but highlights countries that are passing new laws and countries that have strict practices already.

3.1 Studied Countries

We selected Brazil, Netherlands, Kenya, India, and the United States for the following reasons.

Brazil. It has been widely publicized that Brazil is actively trying to avoid having their traffic transit the United States. They have been building IXPs, deploying underwater cables to Europe, and pressuring large U.S. companies to host content within Brazil [8–13, 15, 31]. This effort to avoid traffic transitting a specific country led us to investigate whether their efforts have been successful or not.

Netherlands. We selected to study the Netherlands for three reasons: 1) the Netherlands is beginning to emerge as a site where servers are located for cloud services, such as Akamai, 2) the Netherlands is where a large IXP is located (AMS-IX), and 3) they are drafting a mass surveillance law [41]. Analyzing the Netherlands will allow us to see what effect AMS-IX and the emergence of cloud service hosting has on their traffic.

Kenya. Prior research on the interconnectivity of Africa [23, 29] led us to explore the characterization of an African country's interconnectivity. We chose Kenya for a few reasons: 1) it is a location with many submarine cable landing points, 2) it has high Internet access and usage (for the East African region), and 3) it has more than one IXP [2, 54].

India. India has one of the highest number of Internet users in Asia, second only to China, which has already been well-studied [55, 58]. With such a high number of Internet users, and presumably a large amount of Internet traffic, we study India to see where this traffic is going.

United States. We chose to study the United States because of how inexpensive it is to host domains there, the prevalence of Internet and technology companies located there, and because it is a known surveillance state.

3.2 Countries to Avoid

When analyzing which countries Internet traffic traverses, special attention should be given to countries that may be unfavorable because of their laws and current practices. Some of the countries that are currently conducting surveillance are the "Five Eyes" [22, 37] (the United States, Canada, United Kingdom, New Zealand, and Australia), as well as France, Germany, Poland, Hungary, Russia, Ukraine, Belarus, Kyrgyzstan, and Kazakhstan. On the other hand, countries, such as China, Iran, and

	Collecting Metadata (Phone, Internet)	Requiring ISPs to Participate	No Need for Court Order	Targeted Surveillance
France	✓ [21, 24]	✓ [24]		
Germany	✓ [27]			
UA Emirates				✓ [26]
Bahrain				✓ [4]
Australia	✓ [22]			
New Zealand	✓ [22]			
Canada	✓ [22]			
United States	✓ [22]			
Great Britain	✓ [22]			
Poland	✓ [21]		✓ [21]	
Hungary	✓ [21]		✓ [21]	
Ukraine	✓ [21]	✓ [44, 51]		
Belarus	✓ [21]	✓ [44, 51]		
Kyrgyzstan	✓ [21]	✓ [44, 51]		
Kazakhstan	✓ [21]	✓ [44, 51]		
Russia	✓ [21]	✓ [44, 51]		

Table 1: *Some countries that actively conduct surveillance.*

Russia, are censoring, blocking, and interfering with any traffic that crosses their borders.

Five Eyes. The "Five Eyes" participants are the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB) [22]. According to the original agreement, the agencies can: 1) collect traffic; 2) acquire communications documents and equipment; 3) conduct traffic analysis; 4) conduct cryptanalysis; 5) decrypt and translate; 6) acquire information about communications organizations, procedures, practices, and equipment. The agreement also implies that all five countries will share all intercepted material by default. The agencies work so closely that the facilities are often jointly staffed by members of the different agencies, and it was reported "that SIGINT customers in both capitals seldom know which country generated either the access or the product itself." [37].

A number of other countries are passing laws to facilitate mass surveillance. These laws have differing levels of intensity, which can be seen in Table 1; the countries with the least intense surveillance laws are listed at the top of the table, and those with the more intense laws are listed at the bottom. These countries, along with the "Five Eyes" participants should be flagged when characterizing transnational detours in the following section. Another group of countries includes those that block or interfere with content; these are countries that are infamous for censorship: Iran, China, and Russia. These countries should also be flagged when analyzing transnational detours, as these countries are also unfavorable transit countries due to their practices.

4 Characterizing Transnational Detours

In this section, we describe our measurement methods, the challenges in conducting them, and our findings concerning the transnational detours of default Internet paths.

4.1 Measurement Pipeline

Figures 1 and 2 summarizes our measurement process, which the rest of this section describes in detail. We analyze traceroute measurements to discover which countries are on the path from a client in a particular country to a popular domain. Using traceroutes to measure transnational detours is new; prior work used BGP routing tables to *infer* country-level paths [35]. Because we conduct active measurements, which are limited by our resources, we make a tradeoff and study five countries, as opposed to all countries' Internet paths. We report on measurements that we conducted on January 31, 2016.

4.1.1 Resource Limitations

The iPlane [39] and Center for Applied Internet Data Analysis (CAIDA) [17] projects maintain two large repositories of traceroute data, neither of which turn out to be suitable for our study. iPlane measurements use PlanetLab [46] nodes and has historical data as far back as 2006. Unfortunately, because iPlane uses PlanetLab nodes, which mostly use the Global Research and Education Network (GREN), the traceroutes from PlanetLab nodes will not be representative of typical Internet users' traffic paths [6]. CAIDA runs traceroutes from different vantage points around the world to randomized destination IP addresses that cover all /24s; in contrast, we focus on paths to popular websites from a particular country.

In contrast to these existing studies, we run active measurements that would represent paths of a typical Internet user. To do so, we run DNS and traceroute measurements from RIPE Atlas probes, which are hosted all around the world and in many different settings, including home networks [48]. RIPE Atlas probes can use the local DNS resolver, which would give us the best estimate of the traceroute destination.

Yet, conducting measurements from a RIPE Atlas probe costs a certain amount of "credits", which restricts the number of measurements that we could run. RIPE Atlas also imposes rate limits on the number of concurrent measurements and the number of credits that an individual user can spend per day. We address these challenges in two ways: (1) we reduce the number of necessary measurements we must run on RIPE Atlas probes by conducting traceroute measurements to a single IP address in each /24 (as opposed to all IP address returned by DNS) because all IP addresses in a /24 belong to the same AS, and should therefore be located in the same geographic area; (2) we use a different method—VPN connections—

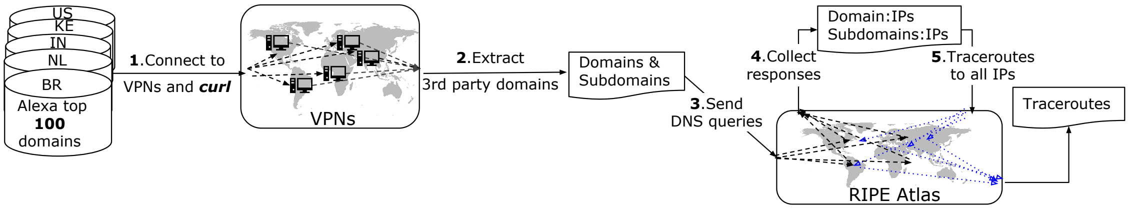


Figure 1: *Measurement pipeline to study Internet paths from countries to popular domains.*

to obtain a vantage point within a foreign country, which is still representative of an Internet user in that country.

4.1.2 Path Asymmetry

The reverse path is just as important as (and often different from) the forward path. Previous work has shown that paths are not symmetric most of the time—the forward path from point A to point B does not match the reverse path from point B to point A [30]. Most work on path asymmetry has been done at the AS level, but not at the country level. Our measurements consider only the forward path (from client to domain or relay), not the reverse path from the domain or relay to the client.

We measured path asymmetry at the country granularity. If country-level paths are symmetric, then the results of our measurements would be representative of the forward *and* reverse paths. If the country-level paths are asymmetric, then our measurement results only provide a lower bound on the number of countries that could potentially conduct surveillance. Using 100 RIPE Atlas probes located around the world, and eight Amazon EC2 instances, we ran traceroute measurements from every probe to every EC2 instance and from every EC2 instance to every probe. After mapping the IPs to countries, we analyzed the paths for symmetry. First, we compared the set of countries on the forward path to the set of countries on the reverse path; this yielded about 30% symmetry. What we wanted to know is whether or not the reverse path has more countries on it than the forward path. Thus, we measured how many reverse paths were a subset of the respective forward path; this was the case for 55% of the paths. This level of asymmetry suggests that our results represent a lower bound on the number of countries that transit traffic; our results are a lower bound on how many unfavorable countries transit a client's path. It also suggests that while providing lower bounds on transnational detours is feasible, designing systems to completely prevent these detours on both forward and reverse paths may be particularly challenging, if not impossible.

4.1.3 Traceroute Origination and Destination Selection

Each country hosts a different number of RIPE Atlas probes, ranging from about 75 probes to many hundreds. Because of the resource restrictions, we could not use all probes in each of the countries. We selected the set of probes that had unique ASes in the country to get the widest representation of origination (starting) points.

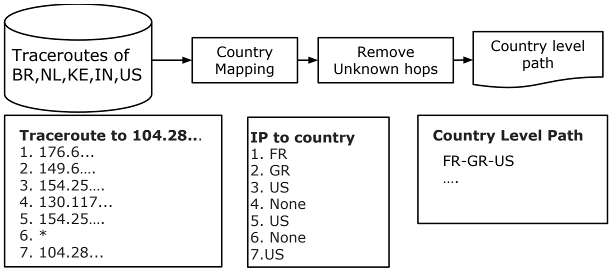


Figure 2: *Mapping country-level paths from traceroutes.*

For destinations, we used the Alexa Top 100 domains in each of the respective countries, as well as the third-party domains that are requested as part of an original web request. To obtain these 3rd party domains we `curl` (*i.e.*, HTTP fetch) each of the Top 100 domains, but we must do so from within the country we are studying. There is no current functionality to `curl` from RIPE Atlas probes, so we establish a VPN connection within each of these countries to `curl` each domain and extract the third-party domains; we `curl` from the client's location in case web sites are customizing content based on the region of the client.

4.1.4 Country Mapping

Accurate IP geolocation is challenging. We use MaxMind's geolocation service to map IP addresses to their respective countries [40], which is known to contain inaccuracies. Fortunately, our study does not require high-precision geolocation; we are more interested in providing accurate lower bounds on detours at a much coarser granularity. Fortunately, previous work has found that geolocation at a country-level granularity is more accurate than at finer granularity [32]. In light of these concerns, we post-processed our IP to country mapping by removing all IP addresses that resulted in a 'None' response when querying MaxMind, which causes our results to provide a conservative estimate of the number of countries that paths traverse. It is important to note that removing 'None' responses will *always* produce a conservative estimate, and therefore we are *always* underestimating

Terminating in Country	Brazil	Netherlands	India	Kenya	United States
Brazil	.169	-	-	-	-
Canada	.001	.007	.015	.006	-
United States	.774	.454	.629	.443	.969
France	.001	.022	.009	.023	.001
Germany	.002	.013	.014	.028	.001
Great Britain	-	.019	.021	.032	.002
Ireland	.016	.064	.027	.108	.001
Netherlands	.013	.392	.101	.200	.024
Spain	.001	-	-	-	-
Kenya	-	-	-	.022	-
Mauritius	-	-	-	.004	-
South Africa	-	-	-	.021	-
United Arab Emirates	-	-	-	.011	-
India	-	-	.053	.002	-
Singapore	-	.002	.103	.027	-

Table 2: *Fraction of paths that terminate in each country by default.*

Transiting Country	Brazil	Netherlands	India	Kenya	United States
Brazil	1.00	-	-	-	-
Canada	.013	.007	.016	.008	.081
United States	.844	.583	.715	.616	1.00
France	.059	.102	.104	.221	.104
Germany	.005	.050	.032	.048	.008
Great Britain	.024	.140	.204	.500	.006
Ireland	.028	.106	.031	.133	.006
Netherlands	.019	1.00	.121	.253	.031
Spain	.176	.004	-	-	-
Kenya	-	-	-	1.00	-
Mauritius	-	-	-	.322	-
South Africa	-	-	-	.334	-
United Arab Emirates	-	-	-	.152	-
India	-	-	1.00	.058	-
Singapore	-	.002	.270	.040	.003

Table 3: *Fraction of paths that each country transits by default.*

the amount of potential surveillance. Figure 2 shows an example of this post-processing.

4.2 Results

Table 2 shows the five countries we studied along the top of the table, and the countries that host their content along in each row. For example, the United States is the endpoint of 77% of the paths that originate in Brazil. A "-" represents the case where no paths ended in that country. For example, no Brazilian paths terminated in South Africa. Table 3 shows the fraction of paths that transit (or end in) certain countries, with a row for each country that is transited.

Finding 4.1 (Hosting Diversity)**:** *About half of the top domains in each of the five countries studied are hosted in a single country. The other half are located in two or more different countries.*

First we analyze hosting diversity; this shows us how many unique countries host a domain. The more countries that a domain is hosted in creates a greater chance that the content is replicated in a favorable country, and could potentially allow a client to circumvent an unfavorable country. We queried DNS from 26 vantage points around the world, which are shown in Figure 3; we chose this set of locations because they are geographically diverse. Then we mapped the IP addresses in the DNS responses to their respective countries to determine how many unique countries a domain is hosted in. Figure 4 shows the fraction of domains that are hosted in different numbers of countries; we can see two common hosting cases: 1) CDNs, and 2) a single hosting country. This shows that many domains are hosted in a single unique country, which leads us to our next analysis—where are these domains hosted, and which countries are traversed on the way to reach these locations.

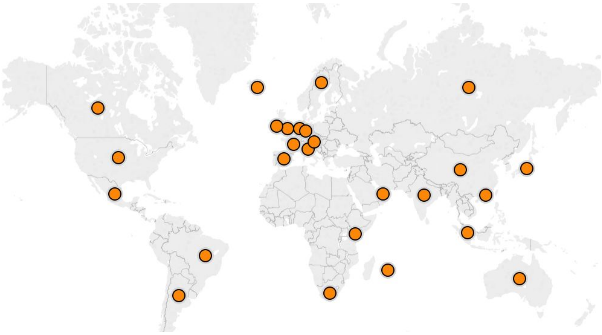
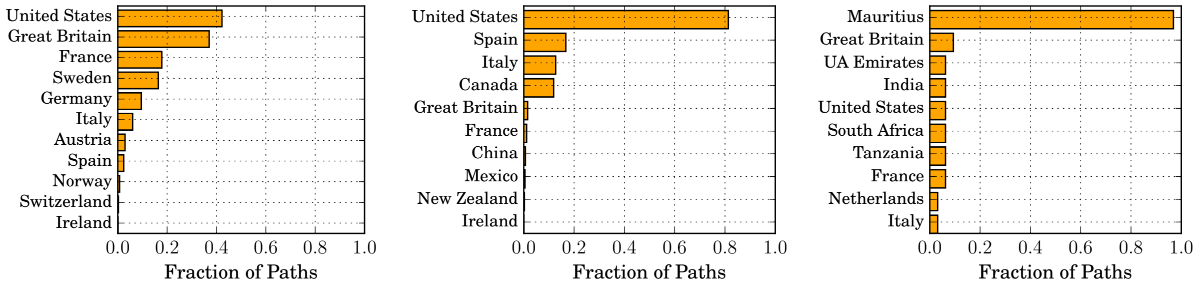


Figure 3: *The locations of vantage points in measuring hosting diversity.*

Finding 4.2 (Domain Hosting)**:** *The most common destination among all five countries studied is the United States: 77%, 45%, 63%, 44%, and 97% of paths originating in Brazil, Netherlands, India, Kenya and the United States, respectively, are currently reaching content located in the United States.*

Table 2 shows the fraction of paths that are hosted in various countries. Despite the extent of country-level hosting diversity, the majority of paths from all five countries terminate in a single country: the United States, a known surveillance state. Our results also show the Netherlands is a common hosting location for paths originating in the Netherlands, India, and Kenya.

Finding 4.3 (Domestic Traffic)**:** *All of the countries studied (except for the United States) host content for a small percentage of the paths that originate in their own country; they also host a small percentage of their respective country-code top-level domains.*



(a) *The Netherlands.* **(b)** *Brazil.* **(c)** *Kenya.*

Figure 5: *The countries that tromboning paths from the Netherlands, Brazil, and Kenya transit.*

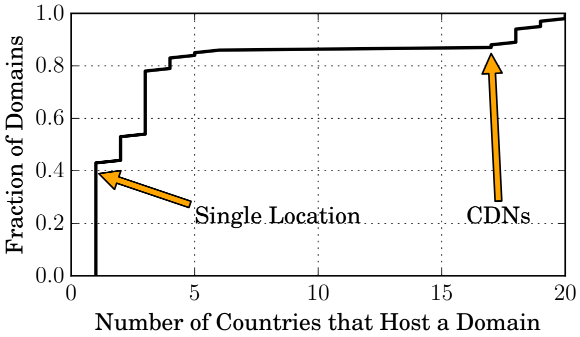


Figure 4: *The number of Alexa Top 100 US Domains hosted in different countries.*

Only 17% of paths that originate in Brazil also end there. Only 5% and 2% of Indian and Kenyan paths, respectively, end in the originating country. For Kenya, 24 out of the Top 100 Domains are .ke domains, and of these 24 domains only 5 are hosted within Kenya. 29 out of 40 .nl domains are hosted in the Netherlands; 4 of 13 .in domains are hosted in India; 18 of 39 .br domains are hosted in Brazil. Interestingly, all .gov domains were hosted in their respective country.

Finding 4.4 (Transit Traffic)**:** *Surveillance states (specifically the United States and Great Britain) are on the largest portion of paths in comparison to any other (foreign) country.*

84% of Brazilian paths traverse the United States, despite Brazil's strong efforts to avoid United States surveillance. Although India and Kenya are geographically distant, 72% and 62% of their paths also transit the United States.

Great Britain and the Netherlands are on the path for a significant percentage of paths originating in India and Kenya: 50% and 20% of paths that originate in Kenya and India, respectively, transit Great Britain. Many paths likely traverse Great Britain and the Netherlands due to the presence of large Internet Exchange Points (*i.e.*, LINX, AMS-IX). Mauritius, South Africa, and the United Arab Emirates transit 32%, 33%, and 15% of paths from Kenya. There are direct underwater cables from Kenya to Mauritius, and from Mauritius to South Africa [53]. Additionally, there is a cable from Mombasa, Kenya to Fujairah, United Arab Emirates, which likely explains the large fraction of paths that include these countries.

Finding 4.5 (Tromboning Traffic)**:** *Brazilian and Netherlands paths often trombone to the United States, despite the prevalence of IXPs in both countries.*

Figures 5a, 5b, and 5c show the fraction of paths that trombone to different countries for the Netherlands, Brazil, and Kenya. 24% of all paths originating in the Netherlands (62% of domestic paths) trombone to a foreign country before returning to the Netherlands. Despite Brazil's strong efforts in building IXPs to keep local traffic local, we can see that their paths still trombone to the United States. This is due to IXPs being seen as a threat by competing commercial providers; providers are sometimes concerned that "interconnection" will result in making business cheaper for competitors and stealing of customers [47]. It is likely that Brazilian providers see other Brazilian providers as competitors and therefore as a threat at IXPs, which cause them to peer with international providers instead of other local providers. Additionally, we see Brazilian paths trombone to Spain and Italy. We have observed that MaxMind sometimes mislabels IP addresses to be in Spain when they are actually located in Portugal. This mislabelling does not affect our analysis of detours through surveillance states, as we do not highlight either Spain or Portugal as a surveillance state. We see Italy often in tromboning paths because Telecom Italia Sparkle is one of the top global Internet providers [5].

Tromboning Kenyan paths most commonly traverse Mauritius, which is expected considering the submarine cables between Kenya and Mauritius. Submarine cables also explain South Africa, Tanzania, and the United Arab Emirates on tromboning paths.

Finding 4.6 (United States as an Outlier)**:** *The United States hosts 97% of the content that is accessed from within the country, and only five foreign countries—France, Germany, Ireland, Great Britain, and the Netherlands—host content for the other 3% of paths.*

Many of the results find that Brazilian, Netherlands, Indian, and Kenyan paths often transit surveillance states, most notably the United States. The results from studying paths that originate in the United States are drastically different from those of the other four countries. The other four countries host very small amounts of content accessed from their own country, whereas the United States hosts 97% of the content that is accessed from within the country. Only 13 unique countries are ever on a path from the United States to a domain in the top 100 (or third party domain), whereas 30, 30, 25, and 38 unique countries are seen on the paths originating in Brazil, Netherlands, India, and Kenya, respectively.

4.3 Limitations

This section discusses the various limitations of our measurement methods and how they may affect the results that we have reported.

Traceroute accuracy and completeness. Our study is limited by the accuracy and completeness of traceroute. Anomalies can occur in traceroute-based measurements [3], but most traceroute anomalies do not cause an overestimation in surveillance states. The incompleteness of traceroutes, where a router does not respond, causes our results to underestimate the number of surveillance states, and therefore also provides a lower bound on surveillance.

IP Geolocation vs. country mapping. Previous work has shown that there are fundamental challenges in deducing a geographic location from an IP address, despite using different methods such as DNS names of the target, network delay measurements, and host-to-location mapping in conjunction with BGP prefix information [45]. While it has been shown that there are inaccuracies and incompleteness in MaxMind's data [32], the focus of this work is on measuring and avoiding surveillance. We use Maxmind to map IP to country (as described in Section 4.1.4), which provides a lower bound on the amount of surveillance, as we have described.

IPv4 vs. IPv6 connectivity. The measurements we conducted only collect and analyze IPv4 paths, and therefore all IPv6 paths are left out of our study. IPv6 paths likely differ from IPv4 paths as not all routers that support IPv4 also support IPv6. Future work includes studying IPv6 paths and which countries they transit, as well as a comparison of country avoidability between IPv4 and IPv6 paths.

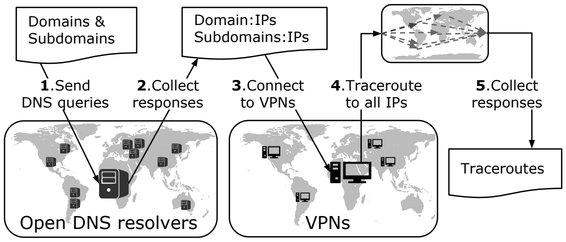


Figure 6: *Measurement approach for country avoidance with open DNS resolvers.*

5 Preventing Transnational Detours

In light of our analysis of the state of default Internet paths from Section 4, we now explore the extent to which various techniques and systems can help clients in various countries prevent unwanted transnational routing detours. We explore two different mechanisms for increasing path diversity: discovering additional website replicas by diverting DNS queries through global open DNS resolvers and creating additional network-layer paths with the use of overlay nodes. We discuss our measurement methods, develop an avoidance metric and algorithm, and present our results.

5.1 Measurement Approach

Country Avoidance with Open Resolvers. If content is replicated on servers in different parts of the world, open DNS resolvers located around the world may also help clients discover a more diverse set of replicas.

Figure 6 illustrates our measurement approach for this study, which differs slightly from that described in Section 4.1: instead of using RIPE Atlas probes to query local DNS resolvers, we query open DNS resolvers located around the world [34]. These open DNS resolvers may provide different IP addresses in the DNS responses, which represent different locations of content replicas. The measurement study in Section 4.1 used RIPE Atlas probes to traceroute to the IP addresses in DNS response; in contrast, for this portion of the study we initiate a VPN connection to the client's country and traceroute (through the VPN connection) to the IP addresses in the DNS responses returned by the open resolvers.

Country Avoidance with Relays. Using an overlay network may help clients route around unfavorable countries or access content that is hosted in a different country. Figure 7 shows the steps to conduct this measurement. After selecting relay machines, we run traceroute measurements from Country X to each relay and from each relay to the set of domains. We then analyze these traceroutes using the pipeline in Figure 2 to determine country-level paths.

We use eight Amazon EC2 instances, one in each geographic region (United States, Ireland, Germany, Singapore, South Korea, Japan, Australia, Brazil), as well as

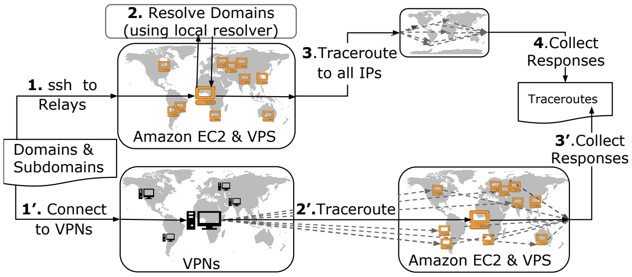


Figure 7: *Measurement approach for country avoidance with overlay network relays.*

4 Virtual Private Server (VPS) machines (France, Spain, Brazil, Singapore), which are virtual machines that are functionally equivalent to dedicated physical servers. The conjunction of these two sets of machines allow us to evaluate surveillance avoidance with a geographically diverse set of relays. By selecting an open resolver in each country that also has a relay in it we can keep the variation in measurement methods low, leading to a more accurate comparison of country avoidance methods.

5.2 Avoidability Metrics

We introduce a new metric and algorithm to measure how often a client in Country X can avoid a specific country Y. Using the proposed metric and algorithm, we can compare how well the different methods achieve country avoidance for any (X, Y) pair.

Avoidability metric. We introduce an avoidability metric to quantify how often traffic can avoid Country Y when it originates in Country X. Avoidability is the fraction of paths that start in Country X and do not transit Country Y. We calculate this value by dividing the number of paths from Country X to domains that do not traverse Country Y by the total number of paths from Country X. The resulting value will be in the range [0,1], where 0 means the country is unavoidable for all of the domains in our study, and 1 means the client can avoid Country Y for all domains in our study. For example, there are three paths originating in Brazil: (1) $BR \rightarrow US$, (2) $BR \rightarrow CO \rightarrow None$, 3) $BR \rightarrow *** \rightarrow BR$. After processing the paths as described in Section 4.1.4, the resulting paths are: (1) $BR \rightarrow US$, (2) $BR \rightarrow CO$, (3) $BR \rightarrow BR$. The avoidance value for avoiding the United States would be 2/3 because two out of the three paths do not traverse the United States. This metric represents a lower bound, because it is possible that the third path timed out ($***$) because it traversed the United States, which would make the third path: $BR \rightarrow US \rightarrow BR$, and would cause the avoidance metric to drop to 1/3.

Avoidability algorithm with open resolvers. Recall from the measurement pipeline for avoidance with open resolvers, described in Section 5.1, that the resulting data are traceroutes from the client in Country X to *all* IP addresses in *all* open DNS resolver responses. To measure avoidability, there must exist at least one path from the client in Country X to the domain for the client to be able to avoid Country Y when accessing the domain. The country avoidance value is the fraction of domains accessible from the client in Country X without traversing Country Y.

Algorithm 1 Avoidability Algorithm

```
function CALCAVOIDANCE(set $paths1$, set $paths2$, string c)
    set $usableRelays$
    for each $(relay, path)$ in $paths1$ do
        if $c$ not in $path$ then
            $usableRelays \leftarrow path$
    set $accessibleDomains$
    for each $(relay, domain, path$ in $paths2$ do
        if $relay$ in $usableRelays$ then
            if $c$ not in $path$ then
                $accessibleDomains \leftarrow domain$
    $D \leftarrow$ number of all unique domains in $paths2$
    $A \leftarrow$ length of $accessibleDomains$
    return $A/D$
```

Avoidability algorithm with relays. Measuring the avoidability of a Country Y from a client in Country X using relays has two components: (1) Is Country Y on the path from the client in Country X to the relay? (2) Is Country Y on the path from the relay to the domain? For every domain, our algorithm checks if there exists at least one path from the client in Country X through any relay and on to the domain, and does not transit Country Y. The algorithm (Algorithm 1) produces a value in the range [0,1] that can be compared to the output of the avoidability metric described above.

Upper bound on avoidability. Although the avoidability metric and algorithm provide a method to quantify how avoidable Country Y is from a client in Country X, it may be the case that a number of domains are only hosted in Country Y, so the avoidance value for these countries would never reach 1.0. For this reason, we measured the *upper bound* on avoidance for a given pair of (Country X, Country Y) that represents the best case value for avoidance. Algorithm 2 shows the pseudocode for computing this metric. The algorithm analyzes the destinations of all domains from all relays and if there exists at least one destination for a domain that is not in Country Y, then this increases the upper bound value. An upper bound value of 1.0 means that every domain studied is hosted (or has a replica) outside of Country Y. This value puts the avoidance values in perspective for each (Country X, Country Y) pair.

Algorithm 2 Avoidance Upper Bound Algorithm

```
function CALCUPPERBOUND(set $relayDomainPaths$, string $c$)
    $zeros(domainLocations)$
    for each $(r,d,p)$ in $relayDomainPaths$ do
        $dest \leftarrow$ last item in $p$
        $domainLocations[d] \leftarrow dest$
    set $accessibleDomains$
    for each $domain$ in $domainLocations$ do
        if $domainLocations[domain] \neq$ set[$c$] then
            $accessibleDomains \leftarrow domain$
    $D \leftarrow$ all unique domains in $relayDomainPaths$
    $A \leftarrow$ length of $accessibleDomains$
    return $A/D$
```

5.3 Results

We compared avoidance values when using open resolvers, when using relays, and when using no country avoidance tool. First, we discuss how effective open resolvers are at country avoidance. We then examine the effectiveness of relays for country avoidance, as well as for keeping local traffic local. Table 4 shows avoidance values; the top row shows the countries we studied and the left column shows the country that the client aims to avoid.

5.3.1 Avoidance with Open Resolvers

A given country is more avoidable (higher avoidance value) when open resolvers are used as a tool for country avoidance.

Finding 5.1 (Open Resolver Effectiveness)**:** *Using open DNS resolvers for country avoidance achieves more country avoidance than using local resolvers and less (or equal) avoidance than using relays for clients in most countries.*

For Brazilian paths, open resolvers only achieve 4% more avoidance than using local resolvers when avoiding the United States, whereas relays achieve 47% more avoidance. On the other hand, open resolvers are about as effective as relays are for avoidance for paths originating in the United States.

Finding 5.2 (Kenya as an Outlier)**:** *For clients in Kenya, open DNS resolvers are significantly more effective than relays for avoiding the United States, South Africa, and the United Arab Emirates.*

Clients in Kenya should use open DNS resolvers when avoiding specific countries, as they can avoid these specific countries more often than when using relays. Kenyan clients can avoid the United States for 55% of paths when using open resolvers, whereas they can only avoid the United States for 40% of paths when using relays. The difference in how often the United States can be avoided can be attributed to the lower amount of DNS diversity when using relays as compared to using open resolvers. For a client in Kenya trying to avoid the United States, the client can only use the relay located in Ireland (because all paths from the client to the other relays traverse the United States), and therefore only gets DNS responses from locally resolving domains on the Ireland relay. When using open resolvers, the client gets more DNS diversity as he gets DNS responses from all open resolvers located in different countries.

The amount of avoidance Kenyan clients can achieve for avoiding South Africa is the same, regardless of whether the client is using relays, because all paths between the client and the relays traverse South Africa. Fortunately, clients can avoid South Africa for significantly more paths when using open resolvers, likely as a result of the fact that open DNS resolvers can better uncover hosting diversity.

5.3.2 Avoidance with Relays

As seen in Table 4, there are two significant trends: 1) the ability for a client to avoid a given Country Y increases with the use of relays, and 2) the least avoidable countries are surveillance states.

Finding 5.3 (Relay Effectiveness)**:** *For 84% of the (Country X, Country Y) pairs shown in Table 4 the avoidance with relays reaches the upper bound on avoidance.*

In almost every (Country X, Country Y) pair, where Country X is the client's country (Brazil, Netherlands, India, Kenya, or the United States) and Country Y is the country to avoid, the use of an overlay network makes Country Y more avoidable than the default routes. The one exception we encountered is when a client is located in Kenya and wants to avoid South Africa, where, as mentioned, all paths through our relays exit Kenya via South Africa.

Finding 5.4 (Relays Achieve Upper Bound)**:** *Clients in the United States can achieve the upper bound of avoidance for all countries—relays help clients in this country avoid all other Country Y in all cases that the domain is not hosted in Country Y.*

Relays are most effective for clients in the United States. On the other hand, it is much rarer for (Kenya, Country Y) pairs to achieve the upper bound of surveillance, showing that it is more difficult for Kenyan clients to avoid a given country. This is not to say that relays are not effective for clients in Kenya; for example, the default routes to the top 100 domains for Kenyans avoid Great Britain 50% of the time, but with relays this percentage increases to about 97% of the time, and the upper bound is about 98%.

Finding 5.5 (Surveillance States are Less Avoidable)**:** *The ability for any country to avoid the United States is significantly lower than it's ability to avoid any other country in all four situations: without relays, with open resolvers, with relays, and the upper bound.*

	No Relay	Open Resolvers	Relays	No Relay	Open Resolvers	Relays	No Relay	Open Resolvers	Relays	No Relay	Open Resolvers	Relays	No Relay	Open Resolvers	Relays
Country to Avoid	*Brazil*			*Netherlands*			*India*			*Kenya*			*United States*		
Brazil	0.00	0.00	0.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Canada	.98	1.00	1.00	.99	1.00	1.00	.98	.98	.98	.99	.99	.99	.92	1.00	1.00
United States	.15	.19	.62	.41	.57	.63	.28	.45	.65	.38	.55	.40	0.00	0.00	0.00
France	.94	.98	1.00	.89	.96	.99	.89	.98	1.00	.77	.89	.98	.89	.99	.99
Germany	.99	.99	1.00	.95	.98	.99	.96	.97	.99	.95	.99	1.00	.99	.99	1.00
Great Britain	.97	.97	1.00	.86	.87	.99	.79	.79	1.00	.50	.71	.97	.99	.99	1.00
Ireland	.97	.98	.99	.89	.97	.99	.96	.99	.99	.86	.98	.99	.99	.99	.99
Netherlands	.98	.98	.99	0.00	0.00	0.00	.87	.98	.99	.74	.98	.99	.97	.99	.99
Spain	.82	1.00	1.00	.99	.99	.99	1.00	.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Kenya	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.00	0.00	0.00	1.00	1.00	1.00
Mauritius	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	.67	.97	.99	1.00	1.00	1.00
South Africa	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	.66	.87	.66	1.00	1.00	1.00
United Arab Emirates	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	.84	1.00	.99	1.00	1.00	1.00
India	1.00	1.00	1.00	.99	1.00	1.00	0.00	0.00	0.00	.94	.94	1.00	.99	1.00	1.00
Singapore	.99	.99	1.00	.99	.99	1.00	.73	.92	.94	.96	.96	1.00	.99	.99	1.00

Table 4: *Avoidance values for different techniques of country avoidance. The upper bound on avoidance is 1.0 in most cases, but not all. It is common for some European countries to host a domain, and therefore the upper bound is slightly lower than 1.0. The upper bound on avoidance of the United States is significantly lower than the upper bound on avoidance for any other country; .886, .790, .844, and .765 are the upper bounds on avoidance of the United States for paths originating in Brazil, Netherlands, India, and Kenya, respectively.*

Despite increasing clients' ability to avoid the United States, relays are not as effective at helping clients avoid this country as compared to the effectiveness of the relays at avoiding all other Country Y. Clients in India can avoid the United States more often than clients in Brazil, Netherlands, and Kenya, by avoiding the United States for 65% of paths. Kenyan clients can only avoid the United States 40% of the time even while using relays. Additionally, the upper bound for avoiding the United States is significantly lower in comparison to any other country.

Finding 5.6 (Keeping Local Traffic Local)**:** *Using relays decreased both the number of tromboning paths, and the number of countries involved in tromboning paths.*

For the cases where there were relays located in one of the five studied countries, we evaluated how effectively the use of relays kept local traffic local. This evaluation was possible for Brazil and the United States. Tromboning Brazilian paths decreased from 13.2% without relays to 9.7% with relays; when relays are used, all tromboning paths goes only to the United States. With the use of relays, there was only 1.3% tromboning paths for a United States client, whereas without relays there was 11.2% tromboning paths. For the 1.2% of paths that trombones from the United States, it goes only to Ireland.

5.3.3 Comparing Avoidance Techniques

From the results shown in Table 4, we can see that using open DNS resolvers for country avoidance is, for the most part, less effective than using overlay network relays. Only 4% of the (origin country, country to avoid)-pairs shown in the table have a higher avoidance value when using open resolvers in comparison to overlay network relays; in reality, this percentage is actually much lower as Table 4 is an abbreviated version of the full table (which can be seen at fill this in). For this reason, we design and implement our system, RAN, solely using overlay network relays (and not open DNS resolvers). These few instances where relays were less effective could be remedied by increasing the number and/or geographic diversity of the relays, resulting in the open resolvers providing no additional avoidance after the relays. We discuss the system and the implementation of the relays in further detail in the next few sections.

6 Design Goals

Here we highlight the main goals of RAN, as well as challenges that are out of the scope of this work.

Foreign Country Avoidance. The primary goal of RAN is to avoid a given country when accessing web content. RAN should provide clients a way to route around a specified country, while still being able to access the desired domain.

Usability. RAN should be designed in a way that is accessible to and easy to use by clients around the world. It should require as little effort by the client as possible.

Scalability. This country avoidance system should be able to scale to large numbers of users. Therefore, RAN should be able to handle the addition of relays, as well as be cost-effective in terms of resources required.

Non-goals. There are some challenges that RAN does not attempt to solve. The system does not address the notion of anonymity; it routes around countries (for rea-

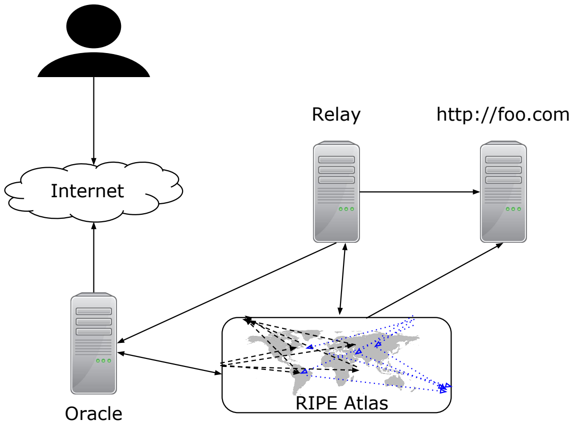


Figure 8: *RAN architecture.*

sons such as avoiding mass surveillance), but it does not attempt to keep users anonymous.

Additionally, RAN does not solve the problem of domestic surveillance (for example, a client in the United States attempting to avoid surveillance by the United States). This is a challenging problem, and asks for future research, but this is out of the scope of our work.

7 Design

In light of the results presented in the previous section, we see that an overlay network can significantly help a client avoid any given country. Therefore, we have designed and developed a system, RAN, that allows users to route around a specified country.

7.1 Architecture

There are three main components to RAN: the oracle, the relays, and the clients. Figure 8 shows which components communicate with eachother and the direction of communication. The relays run as proxy servers in addition to periodically measuring paths from themselves to the top domains that a given client might access and the paths from itself to a location near the given client. The oracle periodically fetches the relay-to-domain paths, as well as calculating various other paths. Using a RIPE Atlas probe in the same country as a client, the oracle can measure: the paths from a location close to the client (which we will refer to as the client from now on) to the relays, and the paths from the client to the domains. Once these paths are mapped to the country level, the oracle can generate and publish a Proxy Autoconfiguration (PAC) file, which allows the client to easily configure their browser to use RAN by specifying the URL where the PAC file resides. The PAC file specifies which proxy to use when accessing a specific domain, or whether or not to use any proxy. More detail are discussed in the following sections.

7.2 Calculating Paths

Given a set of relays that function as proxy servers, it is challenging to measure the necessary country-level paths that will allow the system to specify which proxy to use for a given domain. Here we explain which paths we measure, and how and where they are measured. All of the paths are measured using `traceroute`, which is then mapped to the country level using the same methods as described in Section 4 and shown in Figure 2. The paths we measure are the: forward paths from the client to each relay, forward paths from each relay to each domain, forward paths from the client to each domain, and reverse paths from each relay to the client. The one portion of a path that we cannot measure is the reverse path from each domain to each relay; we cannot measure this because we have no vantage point at or near the domain from which to run `traceroute`.

Client to Relay Paths. As previously mentioned, one of the goals of the system is usability, and therefore, the client should not have to perform almost any actions. To keep the client from having to download any software, the paths from clients to relays are measured using RIPE Atlas probes. A probe is selected from a geographically close location to the client (i.e., the same country), and the oracle triggers the probe to run `traceroute` measurements to each relay in the system. After collecting the responses, the oracle maps the IP-level paths to country-level paths and stores the results.

Relay to Client Paths. The relays are set up with software to run `traceroute` measurements to the IP addresses of RIPE Atlas probes, which represent clients. They then map the responses to country-level paths, and store them locally; the oracle will fetch these paths from each relay.

Relay to Server Paths. The software on the relays also runs `traceroute` measurements to each domain. Similar to the paths to clients, these are mapped to country-level paths, stored, and then fetched by the oracle.

Client to Server Paths. In the case that a path from a client to a domain does not pass through the country specified to avoid *by default*, then none of the proxies should be used. If a proxy is used, then it may actually be causing the path to traverse more countries (unnecessarily). These paths are measured using the RIPE Atlas probes in similar locations as the clients, and the oracle triggers `traceroute` measurements to be run from them to each of the domains. The results are converted to country-level paths and stored on the oracle.

Each of these types of paths must be computed initially, but also re-computed as paths may change. To our knowledge, there has not been any previous work on how often country-level paths change; prior work has explored how often AS-level paths change. To measure how often country-level paths change, we computed the paths from

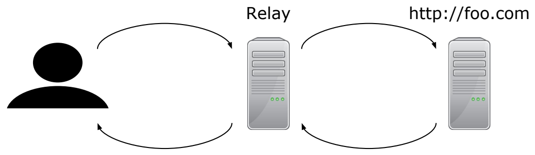


Figure 9: *The path of a web request through a RAN relay, to the domain, and back.*

relays to domains once every two hours and once every hour. On average, the path to X domains changed every two hours, and the path to Y domains changed every one hour. As it takes approximately 30 minutes to compute all paths, RAN re-computes the paths every one hour to incorporate the most recent country-level paths in the system.

As seen in Figure 9, there are four path components when a client accesses web content through RAN. The system measures three out of the four paths; the reverse path from the domains (servers) to the relays is challenging to measure due to a lack of vantage points. Despite not calculating all of the country-level path components, we can show that the country a client is attempting to avoid cannot conduct traffic analysis attacks on the traffic because *at most* the attacker is only on the reverse path from the server to the relay. An attacker would need at least two path components to perform traffic analysis.

7.3 Multiplexing Between Relays

After measuring and aggregating the country-level paths, the oracle decides which relay to use when accessing specific domains from a specific client location. This decision follows three sequential steps:

1. If the default path from the client to the domain does not pass through the specified country, then do not use any of the relays. Otherwise, continue to the next step.
2. For all the paths from the client to the relays, select usable relays such that the path does not contain the specified country.
3. From the set of usable relays, if there is a path from a usable relay to the domain that does not include the specified country, then use that relay for that domain.
4. If there is no path from the client through any of the relays to the domain that does not pass through the specified country, then select the relay that provides the most avoidance (measured by how many other domains it has a path to that avoid the specified country).

The oracle applies this decision process to each domain, and generates a PAC file, which specifies which domains should be accessed through which proxy. A sample PAC file is shown in Listing 1; in this example, proxy 1.2.3.4:3128 should be used when accessing `www.google.com`, but proxy 5.6.7.8:3128 should be used when accessing `www.twitter.com`. Once the PAC file is generated based on the decision chain above, it is published to a URL of the format <client_country>_<country_to_avoid>_pac.pac. The client simply uses this URL to specify their proxy configuration.

Listing 1: *An example PAC file.*

```
function FindProxyForURL(url, host){
    if ((shExpMatch(host, "*.google.com")))
        return "PROXY␣1.2.3.4:3128";
    if ((shExpMatch(host, "*.twitter.com")))
        return "PROXY␣5.6.7.8:3128";
    return "DIRECT";
}
```

As paths are re-computed every hour, the PAC file is also re-computed and published every hour.

7.4 Scaling the System

In addition to usability, another goal of RAN is scalability. The system must support increasing numbers of users.

Adding Relays. As the number of clients increase, their locations may be extremely diverse. This calls for a geographically diverse set of relays, as well as a set of relays that can grow with the number of clients (duplicates in the same locations used to balance the load). RAN is designed in a modular way, and therefore, adding relays is quick, easy, and simple. To add a relay, the system operator must set up a machine as a proxy server, install the RAN relay software, and update the oracle's list of relays. From that point forward, paths will be computed to and from the new relay, and clients will be using it as a proxy.

Adding Oracles. As the number of clients increase, it is possible that a single oracle can not tolerate the computation or storage space necessary for all clients. Adding an oracle is a matter of installing the oracle software on a different machine, and specifying the client locations handled by that oracle (for example, oracle 1 handles all clients in North America and Europe, and oracle 2 handles all clients elsewhere). Both oracles will publish the PAC files to the same server, which causes no changes for the client.

7.5 Fault Tolerance

RAN is resilient to crashed system components, such as a crashed relay or oracle.

Failed Relay. If a relay becomes unresponsive, this issue is handled by the PAC file. The PAC file allows the oracle to specify multiple proxies in a sequential order, such that if the the first proxy fails, then the second proxy is used (and so on). This feature can be used to specify all of the relays that have a path to the domain. And future work can include relay replicas that can be used in the case that a relay crashes.

Failed Oracle. If an oracle crashes, it could trigger a backup oracle to re-compute the PAC files periodically. This is a simple solution because the oracles do not need to convey any information among each other, and therefore, no information is lost. We leave the implementation of backup oracles as future work.

It is worth noting that without backup oracles, clients can still use the system when the oracle fails. The clients will simply be using stale paths, which are likely to be the same original paths, but not always.

8 Implementation

Our prototype implementation of RAN is based on a series of relays, an oracle, and a client. All RAN software can be found at ... I'll add in wherever we end putting it anonymously

Relays. We established nine relays, one in each of the following countries: Brazil, Germany, Singapore, Japan, Australia, France, United States, United Kingdom, and Canada. They are running as Ubuntu Virtual Private Servers (VPSs) with Squid as the proxy server. It is also running the RAN Relay software.

Oracle. The oracle is a Fujitsu RX200 S8 server with dual, eight-core 2.8GHz Intel Xeon E5 2680 v2 processors with 256GB RAM running the Springdale distribution of Linux. It is running the RAN Oracle software.

Client. For the purposes of the system evaluation, we set up a client machine in the Netherlands, which simply accesses web content and uses the PAC file.

9 Evaluation

Using the RAN implementation, we evaluate the system on it's ability to avoid a given country, performance, and scalability in terms of storage and costs.

9.1 Country Avoidance

As the primary goal of the system is to provide country avoidance for a given country, we measured how much avoidance the system achieves. We did so by first calculating the number of *default* paths that avoid a given country. Then we added a single relay, and calculated how many domains the client could access without traversing through the given country. This was repeated for the remaining two relays. The evaluation was conducted under the condition that the client wished to avoid the United States when accessing the Netherlands top 100 domains, and the results are shown in Figure 10.

It is evident that RAN helps a client avoid a foreign country (in this case the United States), as the fraction of domains accessible without traversing the United States without RAN is .46 and with RAN is .63. Additionally, it is clear that adding the first relay provides the greatest increase in provided avoidance, while subsequent relays provide a significantly smaller amount (or no) additional avoidance.

9.2 Performance

A system is not usable if the performance is significantly worse than what a user is accustomed to. To measure the performance of RAN, we `wget` each of the top 100 domains from the client machine in the Netherlands, while using the PAC file. Based on the `wget` output, we calculate the number of seconds to access content using our system. Figure 11 shows the time to access content with RAN in comparison to the time to access the same content without RAN (using default paths).

We can see that the performance of RAN is not significantly worse than that of default paths. In fact, in some cases the performance of RAN is *better* than that of default paths. This could be a result of the relays keeping local traffic local, or due to a closer content replica being selected. These results show that RAN's performance is comparable to the performance of accessing domains without RAN.

9.3 Storage

As the number of clients increase, and subsequently the number of paths being computed increases, the amount of storage must remain reasonable. The storage used by paths can be calculated:

$$Storage(D,R,C) = (DxR) + 2(CxR) + (CxD)$$

D is the number of domains; R is the number of relays; C is representative of the number of clients. While C

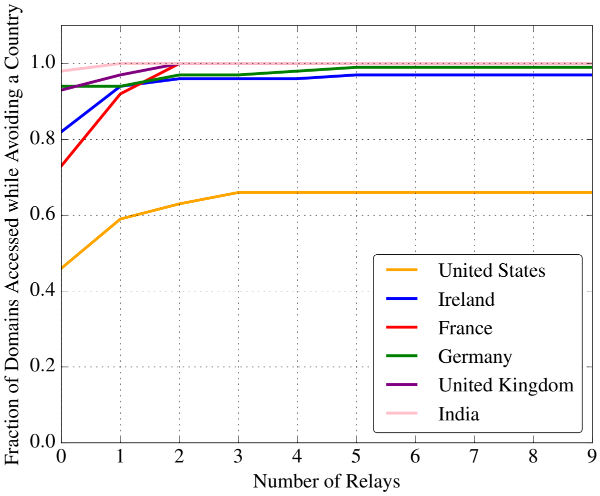


Figure 10: *How much avoidance different numbers and locations of relays achieve.*

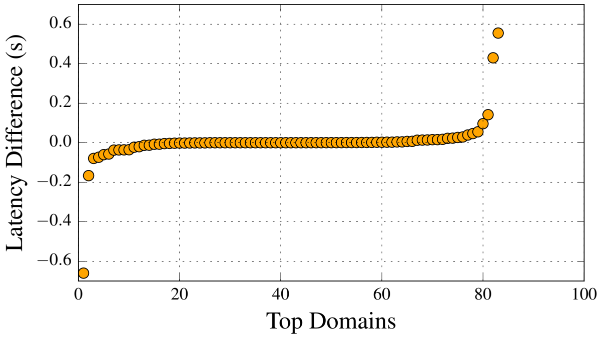


Figure 11: *Latency difference when accessing a webpage via RAN vs. default paths. The difference is calculated by RAN latency minus default latency, and represents the additional latency cost of our system.*

represents clients, it is not the number of clients using the system — it is the number of vantage points the system uses to measure paths from client locations. For the prototype with a single client, the storage space for all paths computed is 480KB. As there is a single PAC file for all clients in a country, C will grow much slower than if there was a different PAC file for each individual client. There are 196 countries in the world today, and if paths and a PAC file were generated for each country, with 100 domains, and three relays, the storage would only be 94MB. This provides plenty of storage for increasing the number of domains included in the PAC file or increasing the number of relays in the system.

9.4 Costs

In addition to storage, the cost of the measurements used in the system must be taken into account. RIPE Atlas credits are a limited resource, and therefore we must earn more credits than we are spending on measurements. The cost in credits follows the equation:

$$Credit\_Cost(D,R,C) = COST_{traceroute}((CxR) + (CxD))$$

Currently, the $COST_{traceroute}$ is 60, resulting in a prototype cost of 6,180 credits, but because these paths are updated each hour, then the daily credit cost is 148,320 credits. In return for hosting a RIPE Atlas probe, we earn 216,000 credits per day, which will support our existing prototype. In order to provide for more clients, more domains, or more resources, we can tune the system to re-compute paths less frequently (only when necessary).

10 Discussion

Avoiding multiple countries. We have studied only the extent to which Internet paths can be engineered to avoid a single country. Yet, avoiding a single country may force an Internet path into *other* unfavorable jurisdictions. This possibility suggests that we should also be exploring the feasibility of avoiding multiple surveillance states (*e.g.*, the “Five Eyes”) or perhaps even entire regions. It is already clear that avoiding certain combinations of countries is not possible, at least given the current set of relays; for example, to avoid the US, Kenyan clients rely on the relay located in Ireland, so avoiding both countries is often impossible.

The evolution of routing detours and avoidance over time. Our study is based on a snapshot of Internet paths. Over time, paths change, hosting locations change, IXPs are built, submarine cables are laid, and surveillance states change. Future work can and should involve exploring how these paths evolve over time, and analyzing the relative effectiveness of different strategies for controlling traffic flows.

Isolating DNS diversity vs. path diversity. In our experiments, the overlay network relays perform DNS lookups from geographically diverse locations, which provides some level of DNS diversity in addition to the path diversity that the relays inherently provide. This approach somewhat conflates the benefits of DNS diversity with the benefits of path diversity and in practice may increase clients’ vulnerability to surveillance, since each relay is performing DNS lookups on each client’s behalf. We plan to conduct additional experiments where the client relies on its local DNS resolver to map domains to IP addresses, as opposed to relying on the relays for both DNS resolution and routing diversity.

Additional RAN Features. Additional features can be implemented at the relay to help preserve client privacy. An example would be to use the relay as a mix, or to send out fake traffic to confuse an attacker that may be trying to perform traffic analysis at the relay.

The oracle could add additional steps in the decision chain introduced in Section 7.3 that take into account relay and path loads. For example, if multiple relays provide a path to a domain that do not traverse the specified country, then the decision between the usable proxies could be determined based on current relay load. In addition to load balancing purposes, the oracle could make relay decisions based on performance. For example, if there are multiple usable relays, the decision could be made on how much time it would take to access the content from each of the relays.

Our current implementation of RAN re-computes all paths once per hour. This could be optimized to only re-compute paths when necessary. For example, a BGP monitoring system could be implemented that alerts the oracle to a path change that affects any path currently in the system. This could decrease the cost and computation of the system.

11 Conclusion

We have measured Internet paths to characterize routing detours that take Internet paths through countries that perform surveillance. Our findings show that paths commonly traverse known surveillance states, even when they originate and end in a non-surveillance state. As a possible step towards a remedy, we have investigated how clients can use the open DNS resolver infrastructure and overlay network relays to prevent routing detours through unfavorable jurisdictions. These methods give clients the power to avoid certain countries, as well as help keep local traffic local. Although some countries are completely avoidable, we find that some of the more prominent surveillance states are the least avoidable.

We make country avoidance accessible to Internet users by designing and implementing RAN, which employs overlay network relays to route Internet traffic around a given country. Our evaluation shows that RAN is successful at avoiding countries while performing as well, if not better, than taking default routes.

Our work presents several opportunities for follow-up studies and future work. First, Internet paths continually evolve; we will repeat this analysis over time and publish the results and data on a public website, to help deepen our collective understanding about how the evolution of Internet connectivity affects transnational routes. Second, our analysis should be extended to study the extent to which citizens in one country can avoid groups of countries or even entire regions. Finally, although our results provide strong evidence for the existence of various transnational data flows, factors such as uncertain IP geolocation make it difficult to provide clients guarantees about country-level avoidance; developing techniques and systems that offer clients stronger guarantees is a ripe opportunity for future work.

References

[1] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris. *Resilient Overlay Networks*, volume 35. ACM, 2001.

[2] Assessment of the Impact of Internet Exchange Points – Empirical Study of Kenya and Nigeria. `http://www.internetsociety.org/sites/default/files/Assessment%20of%20the%20impact%20of%20Internet%20Exchange%20Points%20%E2%80%93%20empirical%20study%20of%20Kenya%20and%20Nigeria.pdf`.

[3] B. Augustin, X. Cuvellier, B. Orgogozo, F. Viger, T. Friedman, M. Latapy, C. Magnien, and R. Teixeira. Avoiding traceroute anomalies with Paris traceroute. In *The 6th ACM SIGCOMM Internet Measurement Conference*, pages 153–158. ACM, 2006.

[4] Bahraini Activists Hacked by Their Government Go After UK Spyware Maker. `https://www.wired.com/2014/10/bahraini-activists-go-after-spyware-source/`.

[5] A Baker's Dozen, 2015 Edition. `http://research.dyn.com/2016/04/a-bakers-dozen-2015-edition/`.

[6] S. Banerjee, T. G. Griffin, and M. Pias. The interdomain connectivity of PlanetLab nodes. In *Passive and active network measurement*, pages 73–82. Springer, 2004.

[7] Z. S. Bischof, J. P. Rula, and F. E. Bustamante. In and Out of Cuba: Characterizing Cuba's Connectivity. In *The 2015 ACM Internet Measurement Conference*, pages 487–493. ACM, 2015.

[8] Brasil Internet Exchange Participants Diversity. `http://ix.br/doc/nic.br.ix.br.euro-ix-27th-berlin.20151027-02.pdf`.

[9] Brazil Builds Internet Cable To Portugal To Avoid NSA Surveillance. `http://www.ibtimes.com/brazil-builds-internet-cable-portugal-avoid-nsa-surveillance-1717417`.

[10] Brazil conference will plot Internet's future post NSA spying. `http://www.reuters.com/article/us-internet-conference-idUSBREA3L1OJ20140422`.

[11] Brazil Looks to Break from US Centric Internet. `http://news.yahoo.com/brazil-looks-break-us-centric-internet-040702309.html`.

[12] Brazil to host global internet summit in ongoing fight against NSA surveillance. `https://www.rt.com/news/brazil-internet-summit-fight-nsa-006/`.

[13] Brazil to press for local Internet data storage after NSA spying. `https://www.rt.com/news/brazil-brics-internet-nsa-895/`.

[14] Brazil Winning Internet. `http://research.dyn.com/2014/07/brazil-winning-internet/#!prettyPhoto/1/`.

[15] Brazil's President Tells U.N. That NSA Spying Violates Human Rights. `http://www.usnews.com/news/articles/2013/09/24/brazils-president-tells-un-that-nsa-spying-violates-human-rights`.

[16] S. Brito, M. Santos, R. Fontes, and D. Perez. Dissecting the Largest National Ecosystem of Public Internet eXchange Points in Brazil. 2016.

[17] CAIDA: Center for Applied Internet Data Analysis. `http://www.caida.org/home/`.

[18] Chinese Routing Errors Redirect Russian Traffic. `http://research.dyn.com/2014/11/chinese-routing-errors-redirect-russian-traffic/`.

[19] Deutsche Telekom to Push for National Routing to Curtail Spying. `http://www.businessweek.com/news/2013-10-14/deutsche-telekom-to-push-for-national-routing-to-curtail-spying`.

[20] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. Technical report, DTIC Document, 2004.

[21] EU Disdains U.S. Surveillance, but Seeks Easier Access. `http://www.bna.com/eu-disdains-us-n57982070518/`.

[22] Eyes Wide Open. `https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf`.

[23] R. Fanou, P. Francois, and E. Aben. On the diversity of interdomain routing in africa. In *Passive and Active Measurement*, pages 41–54. Springer, 2015.

[24] France Has a Powerful and Controversial New Surveillance Law. `http://www.recode.net/2015/11/14/11620670/france-has-a-powerful-and-controversial-new-surveillance-law`.

[25] France Must Reject Law that Gives Carte Blanche to Mass Surveillance Globally. https://www.amnesty.org/en/press-releases/2015/09/france-must-reject-law-that-gives-carte-blanche-to-mass-surveillance-globally/.

[26] Freedom on the Net: United Arab Emirates. https://freedomhouse.org/report/freedom-net/2015/united-arab-emirates.

[27] German Bundestag Passes New Data Retention Law. https://lawfareblog.com/german-bundestag-passes-new-data-retention-law.

[28] Gogo Inflight Internet serves up 'man-in-the-middle' with fake SSL. http://www.csoonline.com/article/2865806/cloud-security/gogo-inflight-internet-serves-up-man-in-the-middle-with-fake-ssl.html.

[29] A. Gupta, M. Calder, N. Feamster, M. Chetty, E. Calandro, and E. Katz-Bassett. Peering at the internet's frontier: A first look at ISP interconnectivity in Africa. In *Passive and Active Measurement*, pages 204–213. Springer, 2014.

[30] Y. He, M. Faloutsos, S. Krishnamurthy, and B. Huffaker. On routing asymmetry in the Internet. In *Global Telecommunications Conference. IEEE*, volume 2. IEEE, 2005.

[31] How Brazil Crowdsourced a Landmark Law. http://foreignpolicy.com/2016/01/19/how-brazil-crowdsourced-a-landmark-law/.

[32] B. Huffaker, M. Fomenkov, and K. Claffy. Geocompare: a comparison of public and commercial geolocation databases. *Proc. NMMC*, pages 1–12, 2011.

[33] Investigatory powers bill: snooper's charter lacks clarity, MPs warn. http://www.theguardian.com/law/2016/feb/01/investigatory-powers-bill-snoopers-charter-lacks-clarity-mps-warn.

[34] Internet-Wide Scan Data Repository. https://scans.io/study/washington-dns.

[35] J. Karlin, S. Forrest, and J. Rexford. Nation-state routing: Censorship, wiretapping, and BGP. *arXiv preprint arXiv:0903.3218*, 2009.

[36] Kazakhstan will require internet surveillance back doors. http://www.engadget.com/2015/12/05/kazakhstan-internet-back-door-law/.

[37] S. S. Lander. International intelligence cooperation: an inside perspective 1. *Cambridge Review of International Affairs*, 17(3):481–493, 2004.

[38] D. Levin, Y. Lee, L. Valenta, Z. Li, V. Lai, C. Lumezanu, N. Spring, and B. Bhattacharjee. Alibi Routing. In *The 2015 ACM Conference on Special Interest Group on Data Communication*, pages 611–624. ACM, 2015.

[39] H. V. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani. iPlane: An information plane for distributed services. In *The 7th Symposium on Operating Systems Design and Implementation*, pages 367–380. USENIX Association, 2006.

[40] MaxMind. https://www.maxmind.com/en/home.

[41] Netherlands New Proposal for Dragnet Surveillance Underway. https://edri.org/netherlands-new-proposals-for-dragnet-surveillance-underway/.

[42] D. Nobori and Y. Shinjo. VPN gate: A volunteer-organized public vpn relay system with blocking resistance for bypassing government censorship firewalls. In *The 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, pages 229–241, 2014.

[43] J. A. Obar and A. Clement. Internet surveillance and boomerang routing: A call for Canadian network sovereignty. In *TEM 2013: The Technology & Emerging Media Track-Annual Conference of the Canadian Communication Association (Victoria)*, 2012.

[44] Once a Defender of Internet Freedom, Putin Is Now Bringing China's Great Firewall to Russia. http://www.huffingtonpost.com/andrei-soldatov/putin-china-internet-firewall-russia_b_9821190.html.

[45] V. N. Padmanabhan and L. Subramanian. An investigation of geographic mapping techniques for Internet hosts. In *ACM SIGCOMM Computer Communication Review*, volume 31, pages 173–185. ACM, 2001.

[46] PlanetLab. http://planet-lab.org/.

[47] Promoting the use of Internet Exchange Points (IXPs): A Guide to Policy, Management and Technical Issues. https://www.internetsociety.org/sites/default/files/Promoting%20the%20use%20of%20IXPs.pdf.

[48] RIPE Atlas. https://atlas.ripe.net/.

[49] H. Roberts, D. Larochelle, R. Faris, and J. Palfrey. Mapping local internet control. In *Computer Communications Workshop (Hyannis, CA, 2011), IEEE*, 2011.

[50] Russia Needs More Internet Security Says Putin. http://www.wsj.com/articles/russia-needs-more-internet-security-says-putin-1412179448.

[51] Russia's Surveillance State. http://www.worldpolicy.org/journal/fall2013/Russia-surveillance.

[52] A. Shah and C. Papadopoulos. Characterizing International BGP Detours. Technical Report CS-15-104, Colorado State University, 2015.

[53] TeleGeography Submarine Cable Map. http://www.submarinecablemap.com/.

[54] The East African Marine System. http://www.teams.co.ke/.

[55] L. Tsui. The panopticon as the antithesis of a space of freedom control and regulation of the internet in china. *China information*, 17(2):65–82, 2003.

[56] M. Wählisch, S. Meiling, and T. C. Schmidt. A framework for nation-centric classification and observation of the internet. In *The ACM CoNEXT Student Workshop*, page 15. ACM, 2010.

[57] M. Wählisch, T. C. Schmidt, M. de Brün, and T. Häberlen. Exposing a nation-centric view on the German internet–a change in perspective on AS-level. In *Passive and Active Measurement*, pages 200–210. Springer, 2012.

[58] S. S. Wang and J. Hong. Discourse behind the forbidden realm: Internet surveillance and its implications on china's blogosphere. *Telematics and Informatics*, 27(1):67–78, 2010.

[59] What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate. https://www.teamupturn.com/reports/2016/what-isps-can-see.

[60] S. Zhou, G.-Q. Zhang, and G.-Q. Zhang. Chinese Internet AS-level topology. *Communications, IET*, 1(2):209–214, 2007.