RAN: Routing Around Nation-States

***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 traversing a given country to 38% of studied paths traversing that country. Based on these findings, we design and implement RAN, a lightweight system that 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 relays around the world, released the source code, and provided instructions to allow clients to use the system.**

I. Introduction

When Internet traffic enters a country, it often becomes subject to that country's local laws and policies. As a result, users, ISPs, and governments have more need than ever to determine—and control—which countries their traffic is traversing. Discovering which countries an end-to-end path traverses and providing mechanisms to avoid certain countries may help users avoid the practices and laws of particular countries. One motivation for avoiding a certain geographic region is to evade surveillance and other types of interference. In some cases, avoiding certain countries may also lower costs or improve performance, where technologies that certain countries use (*e.g.*, firewalls, traffic shapers) throttle network traffic speeds.

An increasing number of countries have passed laws that facilitate mass surveillance of networks within their territory [24], [36], [42], [48]. While governments and citizens alike may want to divert their Internet traffic from countries that perform surveillance (notably, the United States [16], [18], [61]), this is a challenging problem with no known, effective solutions. Additionally, previous work has shown that tromboning paths—paths that start and end in the same country, but also traverse a foreign country— are common [30], [62]; both users and ISPs may wish to prevent these international detours for performance and cost reasons.

With the increasing pervasiveness of encryption (and the efforts of Let's Encrypt), Internet security is improving, but defending against large-scale surveillance activities requires not only encryption, but also mechanisms for controlling where traffic goes in the first place: end-to-end encryption conceals some information content, but it does not protect all sensitive information. 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 [68]; migrating a website to HTTPS can be 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 [38]. Recent work studying Internet of Things (IoT) devices has shown that passive network observers can learn sensitive information about users even when traffic is encrypted [2]; this highlights the risks of large-scale surveillance in the IoT ecosystem. DNS traffic is also revealing and is almost never encrypted [68]. Additionally, ISPs often terminate TLS connections, conducting man-in-the-middle attacks on encrypted traffic for network management purposes [28]. And, of course, encryption offers no solution to interference, degradation, or blocking of traffic that a country might perform on traffic that crosses its borders. Finally, a nation-state may collect and store encrypted traffic; if the encryption is defeated in the future, a nation-state may be able to discover the contents of previous communications. This has already been realized, according to documents leaked from the National Security Agency (NSA) and Government Communications Headquarters (GCHQ): "A 10-year NSA program against encryption technologies made a breakthrough in 2010 which made 'vast amounts' of data collected through internet cable taps newly 'exploitable'" [58].

In this paper, we study two questions: (1) Which countries do *default* Internet routing paths traverse?; (2) What methods can help governments (or citizens, ISPs, etc.) better control transnational Internet paths? We *actively measure* the paths originating in twenty countries to the most popular websites in each of these respective countries. Our analysis in this paper focuses on five countries—Brazil, Netherlands, Kenya, India, and the United States—for a variety of reasons. For example, Brazil has made a concerted effort to avoid traversing certain countries such as the United States through extensive buildout of Internet Exchange Points (IXPs) [13]. The Netherlands has one of the world's largest IXPs and relatively inexpensive hosting. Kenya is one of the most well-connected African countries, but it is still thought to rely on connectivity through Europe and North America for many destinations, even content that might otherwise be local (*e.g.*, local newspapers) [15], [22], [23], [30]. We highlight many trends that are common across all of the countries we study; we have also released detailed statistics on all twenty countries that we measure on the project website and intend to update these on a periodic basis.

In contrast to all previous work in this area, we measure router-level forwarding paths, as opposed to analyzing Border Gateway Protocol (BGP) routes [39], [62], which can provide at best only an indirect estimate of country-level paths to popular sites. Although BGP routing can offer some 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 routes from RIPE Atlas probes [59] in each country to the Alexa Top 1000 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.

While using direct measurements provides these benefits, there are a number of challenges associated with determining which countries a client's traffic is traversing. 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. We study twenty 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 III 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.

We first *characterize the current state of transnational Internet routing detours* (Section III). We explore hosting diversity by first measuring the Alexa Top 1000 domains and comparing the location of path endpoints to that of the Alexa Top 100 domains; we find that there is no significant difference between the results in the two domain sets, and therefore focus on the Alexa Top 100 domains *and all third party domains*. We find that only 45% of the Alexa Top 100 domains in Brazil are hosted in more than one country (other countries studied showed similar results); in many cases, that country is one 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. Despite strong efforts made by some countries to ensure their traffic does not transit certain countries [8]–[11], [33], their traffic still does so. For example, 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 the same 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.

Next, we explore the extent to which clients can avoid certain countries to popular destinations (Section IV). We explore two techniques: using the open DNS resolver infrastructure and using overlay network relays to route Internet traffic around an unfavorable country. Our results demonstrate that these techniques can be effective for clients in certain countries; of course, the effectiveness of these approaches naturally depend on where content is hosted for that country and the diversity of Internet paths between ISPs in that country and the respective hosting sites. For example, our results show that clients in Brazil can 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 increase performance by keeping local traffic local: by using relays in the client's country, fewer paths trombone out of the client's country.

Finally, we *design, implement, and deploy RAN, a system that allows a client to access web content while avoiding the traversal of a specified country* (Section V). We implemented RAN for end-users, but ISPs could also deploy RAN proxies to provide country avoidance as a service to its customers. RAN uses a series of overlay network relays to automatically route a client's traffic around a specified country. We evaluate RAN to assess its ability to avoid certain countries, as well as the effect on end-to-end performance. We also discuss the usability and and scalability of the system. Our evaluation shows that RAN can effectively avoid many different countries and introduces minimal performance overhead.

II. Related Work

a) Nation-state routing analysis: Shah and Papadopoulos recently measured international routing detours—paths that originate in one country, cross international borders, and then return to the original country—using public Border Gateway Protocol (BGP) routing tables [62]. The study discovered 2 million detours each month out of 7 billion paths. Our work differs by *actively* measuring Internet paths using traceroute, yielding a more precise (and accurate) measurement of the paths, as opposed to analyzing BGP routes. Obar and Clement analyzed traceroutes that started and ended in Canada, but tromboned through the United States, and argued that this is a violation of Canadian network sovereignty [50]. Karlin *et al.* developed a framework for country-level routing analysis to study how much influence each country has over interdomain routing [39]. This work measures country centrality using BGP routes and AS-path inference; in contrast, our work uses active measurements and measures avoidability of a given country.

b) Mapping national Internet topologies: Roberts *et al.* developed a method for mapping national networks and identifying ASes that act as points of control [60]. Several studies have also characterized network paths *within* a country, including Germany [66], [67] and China [71], or a country's

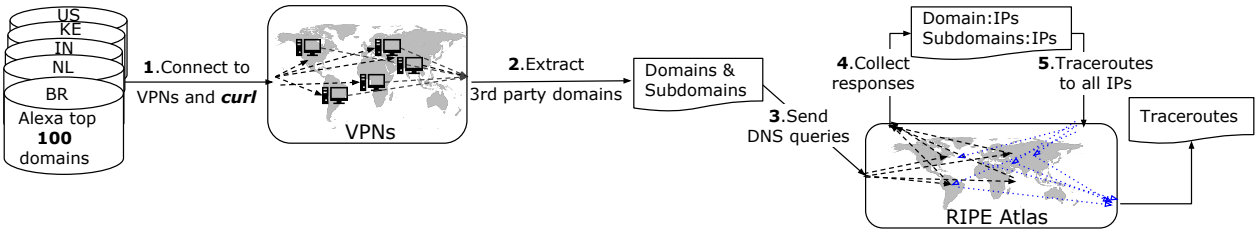


Figure 1: Measurement pipeline to study Internet paths from countries to popular domains.

interconnectivity [6], [22], [30]; these studies focus on intra-country paths, as opposed to focusing on transnational paths.

c) Routing overlays and Internet architectures: Alibi Routing uses round-trip times to prove that that a client's packets did not traverse a forbidden country or region [45], [70]; 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 Network, is an overlay network that routes around failures [1], whereas our overlay network routes around countries. ARROW introduces a model that allows users to route around ISPs [53], but requires ISP participation, making it considerably more difficult to deploy than RAN. ARROW also aims to improve fault-tolerance, robustness, and security, rather than explicitly attempting to avoid certain countries; ARROW provides mechanisms to avoid individual ISPs, but such a mechanism is at a different level of granularity, because an ISP may span multiple countries. Zhang *et al.* presented SCION, a "clean-slate" Internet architecture that provides route control, failure isolation, and explicit trust information for communication [69]; SCION, however, requires fundamental changes to the Internet architecture, whereas RAN is deployable today.

d) Circumvention systems: Certain tools, such as anonymous communications systems or virtual private networks [**?**], [17], [19], [26], [43], [44], [49], [54], [64], [65], may use a combination of encryption and overlay routing to allow clients to avoid surveillance. Tor is an anonymity system that uses three relays and layered encryption to allow users to communicate anonymously [19]. In contrast, RAN does not aim to achieve anonymity; instead, its aim is to ensure that traffic does not traverse a specific country, a goal that Tor cannot achieve. Even tools like Tor do not inherently thwart surveillance: Tor is vulnerable to traffic correlation attacks and some attacks are possible even on encrypted user traffic. VPNGate is a public VPN relay system aimed at circumventing national firewalls [49]. Unfortunately, VPNGate does not allow a client to choose any available VPN, which makes it more difficult for a user to ensure that traffic avoids a particular part of the Internet. Neither of these systems explicitly avoid countries; thus, they may not be able to avoid surveillance or the laws or jurisdiction of a particular country. Additionally, existing circumvention systems generally rely on encryption, which does not prevent surveillance; prior research has shown that websites can be fingerprinted based on size, content, and location of third party resources, which reveals information about the content a user is accessing [68]. Finally, ISPs often execute man-in-the-middle attacks on TLS connections to perform network-management functions [28].

III. 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.

A. Measurement Approach and Challenges

a) Overview of approach: Figure 1 shows the process that we use to discover end-to-end Internet paths from our respective vantage points to various domains. We first use VPNs to establish various vantage points in the countries of interest; then, we use `curl` to download corresponding webpages for each of those popular domains, including all subdomains that are embedded in the site's top-level webpage (1,2). We extract all of these domain names (3) and resolve them to their corresponding IP addresses (4); we then perform traceroutes to each of those IP addresses (5). Figure 2 describes how we translate an IP-level traceroute to a country-level path. We geolocate each IP address, removing unknown hops; we then de-duplicate the country-level path. Although it is seemingly straightforward, this approach entails a number of limitations and caveats, which we describe in the rest of this section.

1) Resource Limitations: We currently focus our measurements on five countries due to resource limitations. The iPlane [46] and Center for Applied Internet Data Analysis (CAIDA) [14] projects maintain large repositories of traceroute data, neither of which are suitable for our study. iPlane has historical data as far back as 2006. Unfortunately, because iPlane uses PlanetLab [55] nodes, which are primarily hosted on the Global Research and Education Network (GREN), iPlane measurements are not be representative of typical Internet users' traffic paths [5]. 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.

Instead, we run active measurements that better 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 in many different types of networks, including home networks [59]. RIPE Atlas probes can use the local DNS resolver, which give us the best estimate of the traceroute destination.

Conducting measurements from a RIPE Atlas probe costs a certain amount of "credits", which restricts the number of measurements that we can 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 addresses 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—to obtain a vantage point within a foreign country, which is still representative of an Internet user in that country.

2) Path Asymmetry: The reverse path (i.e., the path from the server to the client) is just as important as (and often different from) the forward path. Previous work has shown that paths between Internet endpoints are often asymmetric [32]. Most work on path asymmetry has been done at the AS level [25], [31], [32], [52], but not at the country level; our measurements can consider only the forward path (from client to domain or relay), not the reverse path from the domain or relay to the client.

We also (separately) measured path asymmetry at the country granularity. If country-level paths were 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 traffic between two endpoints may traverse. Using 100 RIPE Atlas probes and eight Amazon EC2 instances, we ran traceroute measurements from every probe to every EC2 instance and from every EC2 instance to every probe[1]. After mapping the IP addresses 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; we found that about 30% of the paths were symmetric at the country level. We compared the number of countries on the forward and reverse paths to determine how many reverse paths were a subset of the respective forward path; this situation occurred for 55% of the paths. This level of asymmetry suggests that our results are a lower bound on how many 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 is challenging. If tools that shed light on the reverse path between endpoints (*e.g.*, Reverse Traceroute [41]) see more widespread deployment, the characterizations and avoidance techniques that we develop in this paper could be extended to include reverse paths.

3) Traceroute Origin and Destination Selection: Each country hosts 75 to several hundred RIPE Atlas probes. Because of resource restrictions, we could not use all of the probes in each country. We selected the set of probes that had unique ASes in the country to get the widest representation of origination (starting) points.

To determine how many destinations are representative of the popular sites that client's access, we first compare the country-level paths from a small set of vantage poitns to the Alexa Top 100 domains and to the Alexa Top 1000 domains. The proportion of paths that transited (and ended in) each country are similar in both cases; the paths to the top 1000 domains exhibit a longer tail of countries that transit or host

[1]The EC2 instances were located in the United States, Brazil, Canada, Ireland, Germany, Japan, Australia, and Singapore.

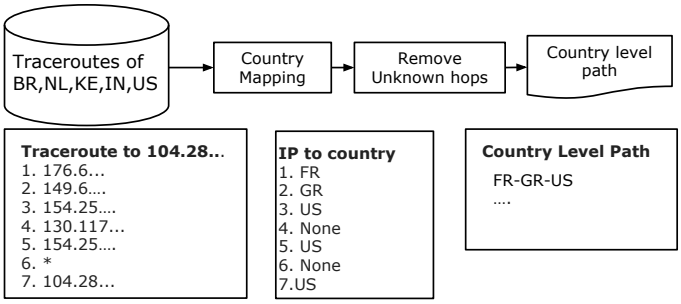


Figure 2: Mapping country-level paths from traceroutes.

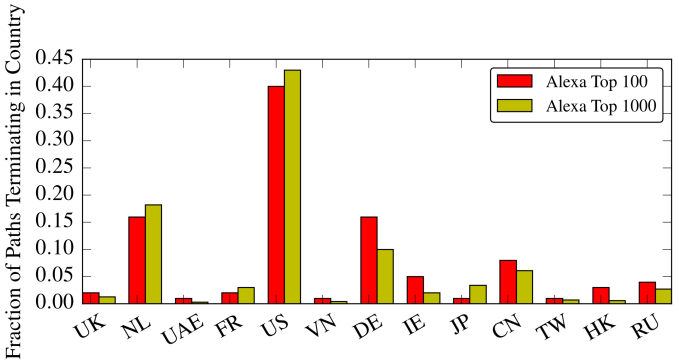


Figure 3: Comparison of path endpoints between the Alexa Top 100 and the Alexa Top 1000.

content, likely because these domains are less popular and therefore hosted in more obscure locations. Otherwise, the results are similar. This comparison can be seen in Figure 3. Therefore, we used the Alexa Top 100 domains in each of the respective countries as our destinations, as well as the third-party domains that are requested as part of an original web request.

To obtain the third-party domains that are hosted on each popular website, we use `curl` to retrieve the homepage for each respective domain from within the country that is hosting the vantage point in question. RIPE Atlas probes do not support these types of Web requests; instead, 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) Country Mapping: Accurate IP geolocation is challenging [20], [21], [27], [29], [34], [40], [56]. We use MaxMind's geolocation service to map IP addresses to their respective countries [47]. Unfortunately, this database is known to contain inaccuracies, particularly for IP addresses that correspond to Internet infrastructure, as opposed to end hosts. Fortunately, previous work has found that geolocation at a country-level granularity is more accurate than at finer granularity [35]. In light of these concerns, we post-processed our IP to country mapping; Figure 2 shows an example of this post-processing. The method starts with 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

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 I: Fraction of paths terminating in a country by default. The fraction in each cell represents the fraction of paths originating in the country at the top of the column and ending in the country indicated in the first cell of the same row.

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 II: Fraction of paths that a country transits by default. The fraction in each cell represents the fraction of paths originating in the country at the top of the column that transit or end in the country indicated in the first cell of the same row.

of countries that paths traverse. It is important to note that removing 'None' responses will *always* produce a conservative estimate.

B. Results

Table I shows five of the countries that we studied along the top of the table and the countries that host their content along in each row. A "-" represents the case where no paths ended in that country. For example, the United States is the endpoint of 77.4% of the paths that originate in Brazil, and no Brazilian paths terminated in South Africa. Table II shows the fraction of paths that transit (or end in) certain countries, with a row

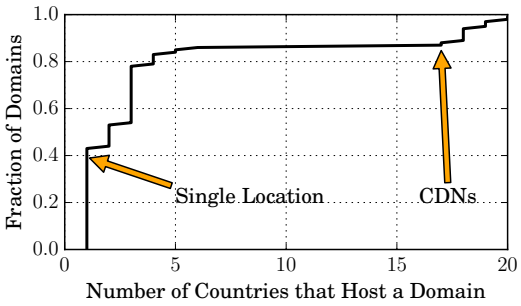


Figure 4: The number of Alexa Top 100 US Domains hosted in different countries.

for each country that is transited. We report on measurements conducted on January 31, 2016, and we are continuing to run these measurements and publish the data.[2]

Finding 3.1 (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.

Hosting diversity reveals how many unique countries host a domain. The more countries host a domain, the greater the likelihood that a client can find a path to that site that avoids a certain country. As a separate measurement experiment, we queried DNS from 26 vantage points around the world, in geographically diverse locations. We then mapped the IP addresses in the DNS responses to countries to determine how many unique countries host a domain. 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.

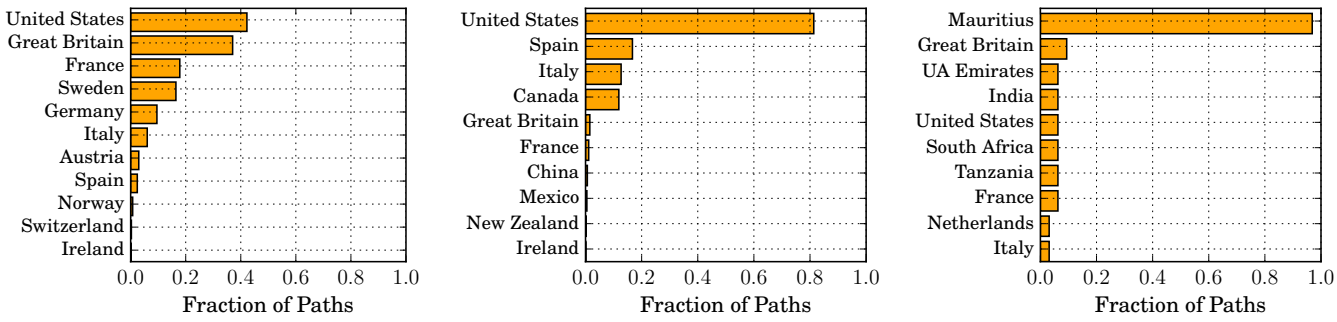
Finding 3.2 (Domain Hosting): The most common destination, regardless of originating country, is the United States.

Table I 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 of the countries we studied terminate in a single country; 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. Our results also show the Netherlands is a common hosting location for paths originating in the Netherlands, India, and Kenya.

Finding 3.3 (Domestic Traffic): All of the countries we 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.

Only 17% of paths that originate in Brazil also end there, and only 5% and 2% of Indian and Kenyan paths, respectively, end in the originating country. For Kenya, 24 out of the Top 100

[2]We have published our data to an anonymized repository at: https://bitbucket.org/ransom_research/data/



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

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

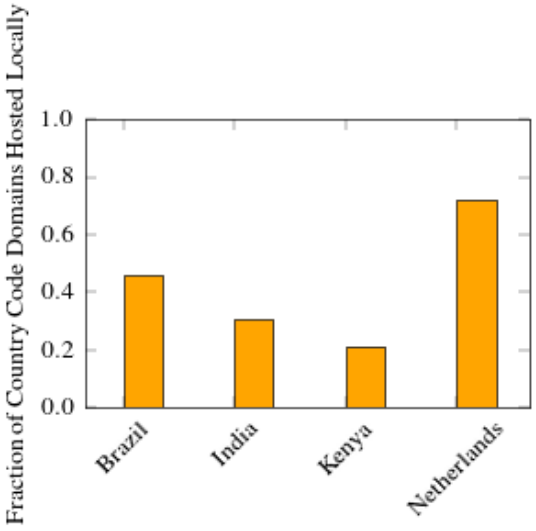


Figure 6: Fraction of country code top-level domains that are hosted locally.

Domains are .ke domains, but only 5 of the 24 are hosted within Kenya. 29 out of 40 .nl domains are hosted in the Netherlands; four of 13 .in domains are hosted in India; 18 of 39 .br domains are hosted in Brazil. Figure 6 shows these results. As one might expect, all .gov domains were hosted in their respective country.

Finding 3.4 (Transit Traffic): 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 [7]–[12]. 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 many of the paths from Kenya and India: 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 [63].

Finding 3.5 (Tromboning Traffic): Brazilian and Netherlands paths often trombone to the United States, despite the prevalence of IXPs in both countries.

Figure 5 shows 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, their paths still trombone to the U.S. 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 [57].

Brazilian providers likely see one another as competitors and therefore as a threat at IXPs, which causes them to peer with international providers instead of other local providers. Additionally, we see Brazilian paths trombone to Spain and Italy. We see Italy often in tromboning paths because Telecom Italia Sparkle is one of the top global Internet providers [4]. MaxMind's geolocation sometimes mislabels IP addresses to be in Spain when they are actually located in Portugal. Despite our inability to disambiguate Spain and Portugal, some of the issues associated with tromboning, such as performance, are still pertinent. We are not aware of specific laws in either of these countries that would make this distinction important from a policy or legal aspect, either.

Tromboning paths that originate in Kenya most commonly traverse Mauritius, which is expected considering the submarine cables between Kenya and Mauritius. Additionally, a cable from Mombasa, Kenya to Fujairah, United Arab Emirates likely explains why many paths include these countries.

Finding 3.6 (United States as an Outlier): The United States hosts 97% of the content that is accessed from within the United States, and only five foreign countries—France, Germany, Ireland, Great Britain, and the Netherlands—host content for the other 3% of paths.

We find that Brazilian, Dutch, Indian, and Kenyan paths often transit the U.S. The results from studying paths that originate in the United States are drastically different from those of the other four countries. The majority of locally popular content in these countries is hosted outside of the respective country, which is shown in Table I; in contrast, 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.

C. Limitations

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

a) 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 states that manipulate or monitor traffic. The incompleteness of traceroutes, where a router does not respond, causes our results to underestimate the number of states that interfere with network traffic.

b) IP geolocation vs. country mapping: 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 [51]. While there are inaccuracies and incompleteness in MaxMind's data [35], the primary motivations for this work are to show that paths are currently going through countries with controversial policies on network interference, and that performance is affected by the paths taken.

c) IPv4 vs. IPv6 connectivity: We collect and analyze only IPv4 paths. IPv6 paths likely differ from IPv4 paths as not all routers that support IPv4 also support IPv6. A comparable study of IP-level paths is an avenue for future work.

IV. Feasibility of Routing Around Nation-States

We now explore the extent to which a system that employs different techniques can help clients avoid specific countries. We explore and evaluate possible methods to (1) increase path diversity with the use of overlay nodes and (2) discover additional website replicas by diverting DNS queries through global open DNS resolvers. In this section, we develop an avoidance metric and algorithm, and evaluate the effectiveness of open resolvers and overlay nodes to avoid specific countries.

A. Measurement Approach

a) 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.

We must use a different measurement approach than that described in the previous section because instead of *locally* resolving the domains, we resolve them using an open resolver. Figure 7 illustrates our measurement approach for this

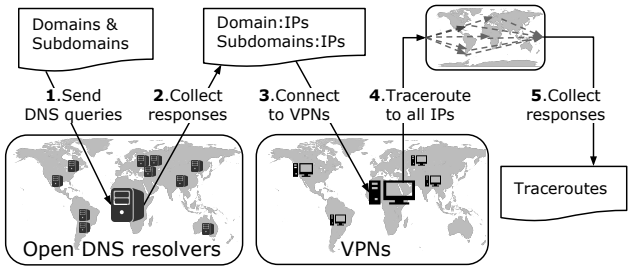


Figure 7: Measurement approach for country avoidance with open DNS resolvers.

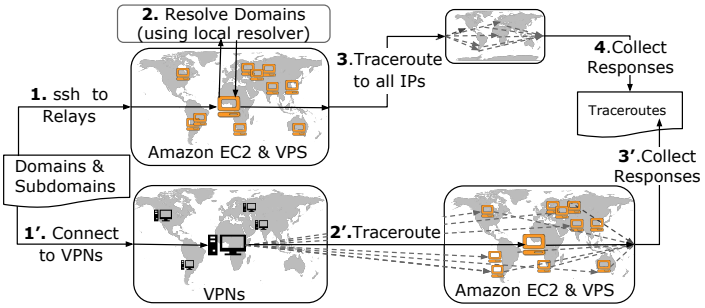


Figure 8: Measurement approach for country avoidance with overlay network relays.

study, which utilizes open DNS resolvers located around the world [37]. 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 III-A 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.

b) Country Avoidance with Relays: An overlay network of relay nodes could help clients route around countries or access content that is hosted in a different country; this section performs measurements to evaluate the feasibility of such an approach. Figure 8 shows the steps in our measurement experiment. After selecting potential relay nodes, we perform traceroute measurements from the country of origin to each relay (1',2'), and from each relay to the set of top 100 domains in the original country (1,2,3). We then analyze these traceroutes using the approach shown in Figure 2 to determine the resulting country-level paths.

We use eight EC2 instances, one in each geographic region (United States, Ireland, Germany, Singapore, South Korea, Japan, Australia, Brazil), as well as four Virtual Private Server (VPS) machines (France, Spain, Brazil, Singapore), which are virtual machines. Combining these two sets of machines allows us to evaluate country 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.

B. Avoidability Metrics

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

a) Avoidability metric: We introduce an avoidability metric to quantify how often traffic can avoid Country Y when it originates in Country X. Avoidability reflects the fraction of paths that originate 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 is 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 III-A4, 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.

b) Avoidability algorithm with open resolvers: Recall from the measurement pipeline for avoidance with open resolvers, described in Section IV-A, 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.

c) Avoidability algorithm with relays: Measuring the avoidability of Country Y from a client in Country X using relays entails 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.

d) Upper bound on avoidability: Although the avoidability metric provides a way to quantify how avoidable Country Y is for a client in Country X, some domains may be hosted only in Country Y, so the avoidance value 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. This algorithm is shown in Algorithm 2; it 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 of 1.0 means that every domain that we measured 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 1 Avoidability Algorithm (with relays). This is the method to calculate the avoidability of a given country when using relays. $paths1$ is the set of country-level paths from client vantage points to relays, $paths2$ is the set of country-level paths from relays to destination domains.

```
1: function CalcAvoidance(set paths1, set paths2, string c)
2:     set suitableRelays
3:     for each (relay, path) in paths1 do
4:         if c not in path then
5:             suitableRelays ← path
6:     set accessibleDomains
7:     for each (relay, domain, path) in paths2 do
8:         if relay in suitableRelays then
9:             if c not in path then
10:                accessibleDomains ← domain
11:    D ← number of all unique domains in paths2
12:    A ← length of accessibleDomains
13:    return A/D
```

Algorithm 2 Avoidance Upper Bound Algorithm. This is the method used to calculate the upper bound on avoidance when using relays. For example, if a domain is solely hosted in a single country, then that country is unavoidable — this algorithm takes this case into account.

```
1: function CalcUpperBound(set relayDomainPaths, string c)
2:     zeros(domainLocations)
3:     for each (r, d, p) in relayDomainPaths do
4:         dest ← last item in p
5:         domainLocations[d] ← dest
6:     set accessibleDomains
7:     for each domain in domainLocations do
8:         if domainLocations[domain] ≠ set[c] then
9:             accessibleDomains ← domain
10:    D ← all unique domains in relayDomainPaths
11:    A ← length of accessibleDomains
12:    return A/D
```

C. Results

We examine the effectiveness of relays for country avoidance, as well as for keeping local traffic local. Table III shows avoidance values; the top row shows the countries we studied and the left column shows the country that the client aims to avoid. Table III shows two trends: (1) the ability for a client to avoid a given Country Y increases with the use of relays; and (2) certain countries such as the United States, the United Kingdom, and other countries that are known to perform interference on traffic are also often the most difficult countries to avoid.

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 4.1 (Open Resolver Effectiveness): Using open DNS resolvers for country avoidance achieves more country avoidance than using local resolvers and no better 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

	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 III: 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.

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.

2) Avoidance with Relays:

Finding 4.2 (Relay Effectiveness): For 84% of the (Country X, Country Y) pairs shown in Table III 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 4.3 (Relays Achieve Upper Bound): Clients in the U.S. can achieve the upper bound of avoidance for all countries—relays help clients in the U.S. avoid all other Country Y unless the domain is 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, 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 4.4 (U.S. is Least Avoidable): The ability for any country to avoid the U.S. is significantly lower than its ability to avoid any other country in all three situations: without relays, with relays, and the upper bound.

Despite increasing the ability to avoid the U.S., relays are less effective at avoiding the U.S. compared to all other Country Y. Clients in India can avoid the U.S. more often than clients in Brazil, Netherlands, and Kenya, by avoiding the U.S. for 65% of paths. Even using relays, Kenyan clients can only avoid the U.S. 40% of the time. Additionally, the upper bound for avoiding the U.S. is significantly lower in comparison to other countries.

Finding 4.5 (Keeping Local Traffic Local): Using relays decreased both the number of tromboning paths, and the number of countries involved in tromboning paths.

Where there were relays located in one of the five studied countries, we evaluated how well the relays kept local traffic local. This evaluation was possible for the U.S. and Brazil. Tromboning Brazilian paths decreased from 13.2% without relays to 9.7% with relays; when relays are used, all tromboning paths go only to the U.S. With the relays, we see only 1.3% tromboning paths for a U.S. client, compared to 11.2% without relays. The 1.2% of paths that trombones from the U.S. go only to Ireland.

3) Comparing Avoidance Techniques: From the results shown in Table III, 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. 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.

V. RAN: Routing Around Nation-States

The previous section showed a first step at demonstrating the extent of the large-scale surveillance problem, and to our

knowledge, there are no existing low-cost, effective countermeasures to this problem. As we have seen an increase in the number of Internet users electing to use anonymity and circumvention systems, such as Tor, we believe that there are Internet users that would also benefit from a system that counters large-scale surveillance.

From our experience conducting measurement studies of Internet paths, we have identified a number of obstacles standing in the way of building such systems. These primarily include a lack of possible measurement methods to learn reverse paths — these are crucial because paths are asymmetric even at the country level — and a lack of knowledge about the locations in which content is replicated.

Some of these obstacles can be completely solved if content providers contributed to the surveillance avoidance system. To address the issue of path asymmetry, the reverse path could be measured from within the provider and used to determine if an unfavorable country is on the reverse path; this could be used in conjunction with our measurements of the forward path. In addition, content providers could strategically publish DNS records such that when a client receives a DNS response, it is for a content replica that allows her to avoid a given country. A content provider could also replicate content in specific regions in order to allow clients to access replicas without traversing a specific country.

We take an approach at designing a system that is a first countermeasure to large-scale surveillance *without* the help of providers. Due to this choice, it is not a perfect system, and it suffers from the obstacles faced during the measurement studies and highlighted in this section. This first system design, called RAN, shows the extent to which we can avoid an unfavorable country without the participation of content providers, and it invites future work and systems that also address the problem of large-scale surveillance.

A. Overview

RAN comprises (1) an overlay network of relays; and (2) an oracle that directs clients to the appropriate relays, as shown in Figure 9. RAN's relays are TCP proxy servers that allow clients to access web content without installing custom software. RAN uses the measurement methods described in Section IV to learn paths between clients, relays, and domains; these results are stored at the oracle, which uses the data to decide which relay a client in some location should use for accessing a certain domain while avoiding a certain country. The oracle periodically computes paths for many combinations of client AS, destination, and country. A client can then query the oracle to determine the appropriate relay to use to avoid a certain country en route to a particular destination.

After describing our threat model and enumerating our design goals for RAN, we explain each component of the system in more detail.

B. Threat Model

RAN addresses an adversary who is restricted to a specific region of the world. The adversary can be passive, and conduct surveillance, or active, and interfere with traffic. We realize that a country's surveillance capabilities are not limited to the infrastructure within its borders, but a country typically can only interfere and manipulate traffic within its borders. For the purposes of this system, we assume the adversary can only view and manipulate traffic within its borders.

An adversary who taps routers around the world, splices undersea fiber cables, or participates in surveillance in foreign states is out of the scope of this work; while RAN does not address this type of attacker, RAN does protect against an attacker, whose interference and monitoring capabilities are limited to a specific land mass.

C. Design Goals

Our measurement results motivate the design and implementation of a relay-based avoidance system, RAN, with the following design goals.

- **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 when accessing a domain. This calls for the role of measurement in the system design and systematizing the measurement methods discussed earlier in the paper.
- **Usability.** RAN should require as little effort as possible from clients. Clients should not have to download or install software, collect any measurements, or understand how the system works. This requires a way for clients to automatically and seamlessly multiplex between relays (proxies) based on different destinations. RAN uses a Proxy Autoconfiguration (PAC) file to support this function. PAC files are supported on many types of devices, including mobile devices (smartphones, tablets, etc.).
- **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. This requires clever measurement vantage points, such that each vantage point is representative of more than one client. The PAC file allows RAN to grow with the number of clients and also supports incremental deployment.
- **Non-goals.** There are some challenges that RAN does not attempt to solve; in particular, it does not provide anonymity; it routes around countries (for reasons that may include avoiding mass surveillance), but it does not attempt to keep users anonymous in the event that traffic can be observed. RAN also does not address domestic interference or surveillance. For example, a client in the United States cannot use RAN to avoid network interference by the United States.

D. Periodic Path Measurement

RAN measures all paths using `traceroute`, which is then mapped to the country level using the same methods as described in Section III 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 portion of the reverse path from the domains to the relays is challenging to measure due to a lack of vantage points in ASes of common destinations. As discussed in Section III-A2, we found that the forward and

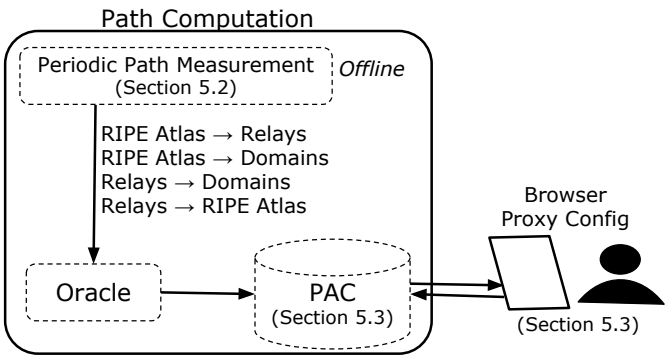


Figure 9: RAN architecture.

reverse paths are asymmetric at the country level, and therefore RAN cannot make any guarantees about which countries are on the path between domains and relays even though it has calculated the paths from relays to domains. Despite the lack of knowledge about this part of the reverse path, we can reason about possible scenarios. If the client's traffic is encrypted, then a country on this part of the reverse path that the client wishes to avoid cannot perform any traffic correlation attacks or website fingerprinting attacks, as the country cannot see who the client is (necessary for website fingerprinting) and does not have access to more than one part of the path (necessary for traffic correlation attacks).

a) Client-to-Relay Paths: To avoid requiring the client to install custom software, RAN measures client-to-relay paths from RIPE Atlas probes that serve as vantage points for the ASes where RAN clients might be. RAN selects probes that are geographically close the client (*e.g.*, in the same country). The oracle triggers the probe to run traceroutes to each relay. After collecting the responses, the oracle maps the IP-level paths to country-level paths and stores the results.

b) Relay-to-Client Paths: The RAN relays perform traceroutes to the IP addresses of RIPE Atlas probes, which represent client ASes. They then derive country-level paths; the oracle learns these paths from each relay.

c) Relay-to-Server Paths: Relays perform traceroutes to each domain. As with paths to clients, relays derive country-level paths and send them to the oracle.

d) Client-to-Server Paths: In case 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. These paths are measured using the RIPE Atlas probes in similar locations as the clients, and the oracle triggers traceroutes from each of them to each of the domains. Corresponding country-level paths are stored at the oracle.

These paths must be 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. We measured the country-level paths from a RIPE Atlas probe to the Alexa Top 100 domains once per day for a month to see how stable country-level paths are. Across the measured domains, we found the average time between path changes to be about five days. Therefore, RAN re-computes the paths every five days to incorporate the most recent country-level paths.

Configuration 1: 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";
}
```

E. PAC File Generation

The oracle follows four steps to decide which relay a client should use to access a specific domain: (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. (2) Otherwise, for all the paths from the client to the relays, select suitable relays, which are relays where the country to avoid is not on the forward or reverse path between the client and relay. (3) From this set, if there is a path from a suitable 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 that avoid the specified country). The oracle applies this decision process to each domain, which results in a mapping of domains to relays that can be used to avoid the given country. To facilitate automatic multiplexing between relays, RAN utilizes Proxy Autoconfiguration (PAC) files, which define how browsers should choose a proxy when fetching a URL. In the example PAC file in Configuration 1, 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`. The oracle uses the mapping of domains to relays to generate a PAC file, which specifies which domains should be accessed through which proxy. The PAC file is published online to a URL of the format <client_country>_<country_to_avoid>_pac.pac. The client uses this URL to specify their proxy configuration. Paths are re-computed every five days, so the contents of the PAC file are also updated every five days.

F. Scalability and Fault Tolerance

Adding relays to RAN is straightforward. Additionally, RAN is resilient to failures of system components.

a) Adding relays and oracles: To add a relay, the system operator must set up a machine as a proxy server, install the relay software, and update the oracle's list of relays. From that point onward, paths will be computed to and from the new relay, and clients will begin using the new proxy. Adding an oracle requires installing the oracle software on a different machine, and specifying the client locations handled by that oracle (*e.g.*, one oracle handles clients in North America and Europe, and another handles clients elsewhere). Both oracles will publish the PAC files to the same server, which causes no changes for the client.

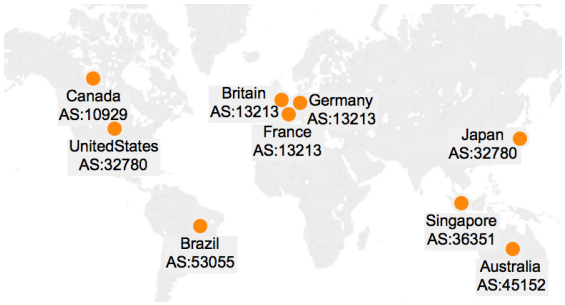


Figure 10: The locations and ASNs for RAN relays.

b) Failed relays and oracles: Unresponsive relays are 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 client users the second proxy (and so on). This feature can be used to specify all of the relays that have a path to the domain. Among other mechanisms, we can detect a failed oracle by determining that its PAC file is older than one hour. Detecting a failed oracle could trigger a backup oracle to re-compute the PAC files periodically. Because oracles are stateless, failover is straightforward. Without backup oracles, clients can still use the system when the oracle fails. The clients will simply be using stale paths, which are likely (but not guaranteed) to be functional, since country-level paths change infrequently.

G. Implementation and Deployment

Our implementation of RAN includes relays, an oracle, and a client. RAN is open source and written in Python; the oracle is written in just 175 lines of code and the relay is written in just under 200 lines of code. RAN is currently deployed globally, and any user may use it today.[3]

We assume that users and machines are trustworthy, and therefore the system runs securely. This implementation of RAN allows a client to avoid a single country at a time; attacks on RAN, such as Denial of Service attacks and targetted surveillance of the relays, are outside the scope of the paper.

a) Relays: The current deployment has ten relays, one in each of the following countries: Brazil, Germany, Singapore, Japan, Australia, France, United States, United Kingdom, Netherlands, and Canada; Figure 10 shows these relay locations, along with their corresponding ASes. These relays operate as Ubuntu Virtual Private Servers (VPSes) with Squid as the proxy server and the RAN Relay software.

b) Oracle: The oracle software runs on a Fujitsu RX200 S8 server with dual, eight-core 2.8 GHz Intel Xeon E5 2680 v2 processors with 256GB RAM running RedHat Linux.

c) Client: To evaluate the RAN deployment, we set up a client machine in the Netherlands, which simply accesses web content and uses the PAC file generated by the oracle.

[3]We have released an anonymized source code repository, complete with usage instructions, at: https://bitbucket.org/ransom_research/ran/

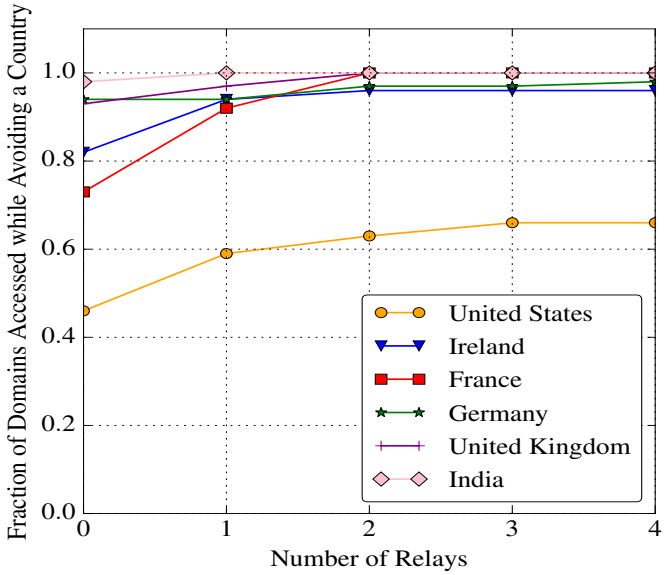


Figure 11: The effect of the number of relays on avoidance, for a client in the Netherlands. We tested RAN with up to nine relays.

VI. Evaluation

We evaluate RAN's ability to avoid a given country, its performance, and its storage and measurement costs.

A. Country Avoidance

We measured RAN's effectiveness in achieving country avoidance. 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. We repeated this approach for the remaining relays. We conducted the evaluation under the condition that the client wished to avoid different countries when accessing the Netherlands top 100 domains; Figure 11 shows these results. Each line represents the fraction of domains accessible while avoiding the country that the line represents. For example, 46% of domains are accessible without traversing the U.S. when RAN is not being used (zero relays), and if RAN is used, then 63% of domains are accessible without traversing the U.S.

RAN helps a client avoid a foreign country, as the fraction of domains accessible without traversing the specified country without RAN is lower than with RAN. Additionally, adding the first relay provides the greatest benefit, while subsequent relays offer diminishing returns. Figure 11 clearly shows that avoiding the U.S. is much more difficult (or impossible) than any other country. Only 63% of domains can be accessed while avoiding the U.S., whereas almost all domains can be accessed while avoiding any other given country.

It is important to note that RAN cannot guarantee that a country is avoided because for some domains, the path must go through the unfavorable country, as evidenced by our results for avoiding the United States. Despite this lack of guarantees, the system reduces the number of requests

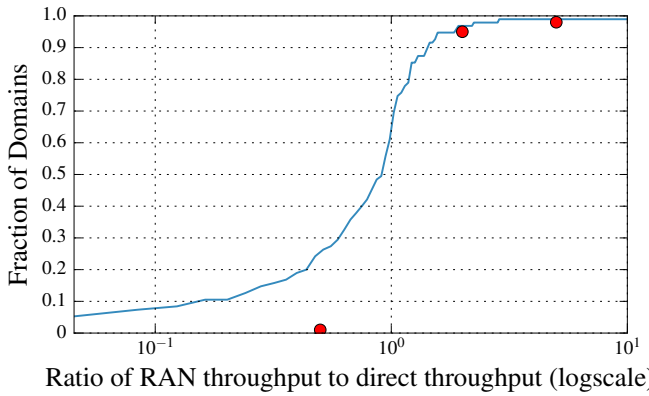


Figure 12: The ratio of RAN throughput to direct throughput. The points on the graph show measurements from the Resilient Overlay Networks (RON [1]) system and thus represent the performance of overlay network that is solely designed to improve reliability.

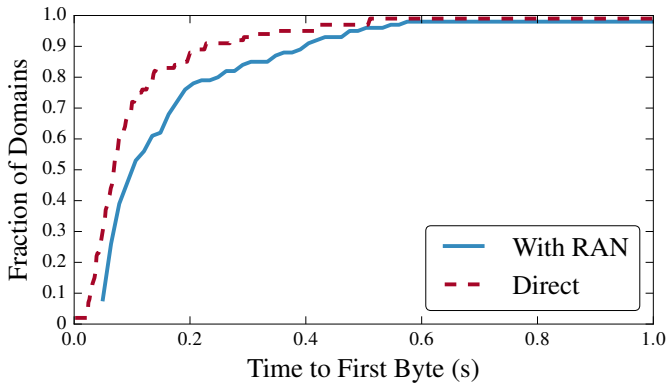


Figure 13: Time to First Byte for RAN and direct paths.

that transit the unfavorable country; additionally, the client can learn which domains are not accessible without passing through the unfavorable country, and can then decide whether or not to fetch that page.

B. Performance

To measure the performance of RAN, we measure both the throughput and latency.

To measure throughput, we ran `wget` for each of the top 100 domains from the client machine in the Netherlands using an oracle-generated PAC file. Because different relays could have been used to avoid a single domain, the oracle selected a random relay from those that would allow the client to avoid the country. The oracle generated ten PAC files for a client in the Netherlands who wishes to avoid the United States, randomly selecting a relay for domains that could have used different relays, and `wget` was used for the top 100 domains for each PAC file generated. Based on the `wget` output, we calculate the number of seconds to access content using our system and take the average across the ten experiments.

Figure 12 shows a CDF of the ratio of RAN throughput to direct throughput. The throughput of RAN is not significantly worse than that of default paths. In some cases the performance of RAN is *better* than that of default paths. Such improvements 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. Figure 12 also compares RAN's throughput to RON's throughput, illustrated with the red dots; these data points are taken directly from the RON paper [1]. RAN performs worse than RON ($x < 1$), which is expected, as the detours that RAN introduces inherently inflate paths. Interestingly, both RON and RAN improve throughput for a similar fraction of samples ($x > 1$).

To measure the latency of RAN, we ran `curl` to each of the top 100 domains from the client in the Netherlands, using the ten oracle-generated PAC files to allow the client to select the appropriate relays. This experiment allowed us to measure the time to first byte (TTFB) for web downloads; we found the average TTFB when accessing content using RAN and found the TTFB when using direct paths; Figure 13 shows these results. The median TTFB for direct paths is 68.5 ms; for RAN paths the median is 100.8 ms; 90th percentile TTFB is 22.5 ms and 40.4 ms, respectively.

C. Storage and Measurement Costs

As the number of clients increases, and hence the number of paths being computed increases, the amount of storage must remain reasonable. The storage used by paths can be calculated as $DR + 2CR + CD$ where D is the number of domains; R is the number of relays; and C is the number of ASes from which RAN measures. The storage required for a single client, 100 domains, and nine relays is 480 KB. Because 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; if RAN computed paths and a PAC file for each country, with 100 domains, and three relays required storage would be only 94 MB, making it feasible to increase the number of relays and domains.

RIPE Atlas credits are also a limited resource. Cost is proportional to $C \cdot (R + D)$. Each traceroute costs 60 RIPE Atlas credits, so one set of measurements for one client, 100 domains, and nine relays costs 6,180 credits; 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. To provide for more clients, more domains, or more resources, we can tune the system to re-compute paths less frequently, as we discuss in Section VII.

VII. Discussion

a) 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. Future work should explore the feasibility of avoiding multiple countries or perhaps even entire regions.

b) Evolution over time: Our study is based on a snapshot of paths. Over time, paths change, hosting locations change, IXPs are built, submarine cables are laid, and the countries conducting network interference change. We are continuing to collect the measurements that we have presented in this paper to facilitate future exploration of how these characteristics evolve over time.

c) 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.

d) ISPs controlling country avoidance: Future work includes modifying RAN to be implemented within an ISP. Adding country avoidance functionality within ISPs (government-controlled or otherwise) allows ISPs to provide this as a transparent service to customers. A government that wishes to control which countries its citizens' traffic is traversing might deploy RAN in the country's ISPs.

e) Additional RAN features: The oracle could add additional steps in the decision chain introduced in Section V-E that take into account relay and path loads. For example, if multiple relays provide a path to a domain that does not traverse the specified country, then the decision between the suitable proxies could be determined based on current relay load or performance. Our current implementation of RAN re-computes all paths once per five days; we could only re-compute paths when necessary. For example, a BGP monitoring system detect routing changes and trigger path measurements.

VIII. Conclusion

We have characterized routing detours that take Internet paths through foreign countries, which may make clients susceptible to foreign surveillance, performance degradation, and increased costs. We find that paths commonly traverse known surveillance states, even when they originate and end in a non-surveillance state. As a first step towards a remedy, we have investigated how clients, ISPs, and governments can use overlay network relays to prevent routing detours through unfavorable jurisdictions. This method gives clients the power to avoid certain countries, as well as help keep local traffic local. We have designed, implemented, and deployed RAN, which employs overlay network relays to route traffic around a given country. Our evaluation shows that RAN can in many cases avoid certain countries while performing nearly as well, if not better, than taking default routes.

References

[1] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris, "Resilient overlay networks," in *ACM Symposium on Operating Systems Principles (SOSP)*, vol. 35, no. 5. ACM, 2001.

[2] N. Apthorpe, D. Reisman, and N. Feamster, "Poster: A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic," 2016.

[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*. ACM, 2006, pp. 153–158.

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

[5] S. Banerjee, T. G. Griffin, and M. Pias, "The Interdomain Connectivity of PlanetLab Nodes," in *Passive and Active Network Measurement*. Springer, 2004, pp. 73–82.

[6] 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*. ACM, 2015, pp. 487–493.

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

[8] "Brazil Conference will Plot Internet's Future Post NSA Spying," http://www.reuters.com/article/us-internet-conference-idUSBREA3L1OJ20140422.

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

[10] "Brazil to Host Global Internet Summit in Ongoing Fight Against NSA Surveillance," https://www.rt.com/news/brazil-internet-summit-fight-nsa-006/.

[11] "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.

[12] "Brazil to Press for Local Internet Data Storage After NSA Spying," https://www.rt.com/news/brazil-brics-internet-nsa-895/, 2013.

[13] S. H. B. Brito, M. A. Santos, R. dos Reis Fontes, D. A. L. Perez, and C. E. Rothenberg, "Dissecting the largest national ecosystem of public internet exchange points in brazil," in *International Conference on Passive and Active Network Measurement*. Springer, 2016, pp. 333–345.

[14] "CAIDA: Center for Applied Internet Data Analysis," http://www.caida.org/home/.

[15] J. Chavula, N. Feamster, A. Bagula, and H. Suleman, "Quantifying the effects of circuitous routes on the latency of intra-africa internet traffic: A study of research and education networks," in *International Conference on e-Infrastructure and e-Services for Developing Countries*. Springer, 2014, pp. 64–73.

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

[17] H. Corrigan-Gibbs, D. Boneh, and D. Mazières, "Riposte: An anonymous messaging system handling millions of users," in *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, 2015, pp. 321–338.

[18] "Deutsche Telekom to Push for National Routing to Curtail Spying," http://www.businessweek.com/news/2013-10-14/deutsche-telekom-to-push-for-national.

[19] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," DTIC Document, Tech. Rep., 2004.

[20] B. Eriksson, P. Barford, B. Maggs, and R. Nowak, "Posit: a lightweight approach for ip geolocation," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 2, pp. 2–11, 2012.

[21] B. Eriksson, P. Barford, J. Sommers, and R. Nowak, "A learning-based approach for ip geolocation," in *Passive and Active Measurement*. Springer, 2010, pp. 171–180.

[22] R. Fanou, P. Francois, and E. Aben, "On the diversity of interdomain routing in africa," in *International Conference on Passive and Active Network Measurement*. Springer, 2015, pp. 41–54.

[23] R. Fanou, G. Tyson, P. Francois, and A. Sathiaseelan, "Pushing the frontier: Exploring the african web ecosystem," in *Proceedings of the 25th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2016, pp. 435–445.

[24] "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/.

[25] L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Transactions on Networking (ToN)*, vol. 9, no. 6, pp. 733–745, 2001.

[26] N. Gelernter, A. Herzberg, and H. Leibowitz, "Two cents for strong anonymity: The anonymous post-office protocol," *Proceedings on Privacy Enhancing Technologies*, vol. 2, pp. 1–20, 2016.

[27] P. Gill, Y. Ganjali, B. Wong, and D. Lie, "Dude, where's that ip?: Circumventing measurement-based ip geolocation," in *Proceedings of the 19th USENIX conference on Security*. USENIX Association, 2010, pp. 16–16.

[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] C. Guo, Y. Liu, W. Shen, H. J. Wang, Q. Yu, and Y. Zhang, "Mining the web and the internet for accurate ip address geolocations," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 2841–2845.

[30] 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*. Springer, 2014, pp. 204–213.

[31] Y. He, M. Faloutsos, and S. Krishnamurthy, "Quantifying routing asymmetry in the internet at the as level," in *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, vol. 3. IEEE, 2004, pp. 1474–1479.

[32] Y. He, M. Faloutsos, S. Krishnamurthy, and B. Huffaker, "On routing asymmetry in the internet," in *Global Telecommunications Conference, 2005. GLOBECOM'05. IEEE*, vol. 2. IEEE, 2005, pp. 6–pp.

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

[34] Z. Hu, J. Heidemann, and Y. Pradkin, "Towards geolocation of millions of ip addresses," in *Proceedings of the 2012 ACM conference on Internet measurement conference*. ACM, 2012, pp. 123–130.

[35] B. Huffaker, M. Fomenkov, and K. Claffy, "Geocompare: A Comparison of Public and Commercial Geolocation Databases," *Proc. NMMC*, pp. 1–12, 2011.

[36] "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.

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

[38] A. Johnson, C. Wacek, R. Jansen, M. Sherr, and P. Syverson, "Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries," in *CCS*. ACM, 2013, http://www.ohmygodel.com/publications/usersrouted-ccs13.pdf.

[39] J. Karlin, S. Forrest, and J. Rexford, "Nation-state Routing: Censorship, Wiretapping, and BGP," *arXiv preprint arXiv:0903.3218*, 2009.

[40] E. Katz-Bassett, J. P. John, A. Krishnamurthy, D. Wetherall, T. Anderson, and Y. Chawathe, "Towards ip geolocation using delay and topology measurements," in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*. ACM, 2006, pp. 71–84.

[41] E. Katz-Bassett, H. V. Madhyastha, V. K. Adhikari, C. Scott, J. Sherry, P. Van Wesep, T. E. Anderson, and A. Krishnamurthy, "Reverse traceroute." in *NSDI*, vol. 10, 2010, pp. 219–234.

[42] "Kazakhstan Will Require Internet Surveillance Back Doors," http://www.engadget.com/2015/12/05/kazakhstan-internet-back-door-law/, 2015.

[43] A. Kwon, H. Corrigan-Gibbs, S. Devadas, and B. Ford, "Atom: Scalable anonymity resistant to traffic analysis," *arXiv preprint arXiv:1612.07841*, 2016.

[44] A. Kwon, D. Lazar, S. Devadas, and B. Ford, "Riffle," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 115–134, 2016.

[45] 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*. ACM, 2015, pp. 611–624.

[46] 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*. USENIX Association, 2006, pp. 367–380.

[47] "MaxMind," https://www.maxmind.com/en/home.

[48] "Netherlands New Proposal for Dragnet Surveillance Underway," https://edri.org/netherlands-new-proposals-for-dragnet-surveillance-underway/, 2015.

[49] 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)*, 2014, pp. 229–241.

[50] 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.

[51] V. N. Padmanabhan and L. Subramanian, "An Investigation of Geographic Mapping Techniques for Internet Hosts," in *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4. ACM, 2001, pp. 173–185.

[52] V. Paxson, "End-to-end routing behavior in the internet," *IEEE/ACM transactions on Networking*, vol. 5, no. 5, pp. 601–615, 1997.

[53] S. Peter, U. Javed, Q. Zhang, D. Woos, T. Anderson, and A. Krishnamurthy, "One tunnel is (often) enough," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 99–110, 2015.

[54] A. Piotrowska, J. Hayes, T. Elahi, S. Meiser, and G. Danezis, "The loopix anonymity system," *arXiv preprint arXiv:1703.00536*, 2017.

[55] "PlanetLab," http://planet-lab.org/.

[56] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye, "Ip geolocation databases: Unreliable?" *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 2, pp. 53–56, 2011.

[57] "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, 2012.

[58] "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[59] "RIPE Atlas," https://atlas.ripe.net/.

[60] H. Roberts, D. Larochelle, R. Faris, and J. Palfrey, "Mapping Local Internet Control," in *Computer Communications Workshop (Hyannis, CA, 2011), IEEE*, 2011.

[61] "Russia Needs More Internet Security Says Putin," http://www.wsj.com/articles/russia-needs-more-internet-security-says-putin-1412179448, 2014.

[62] A. Shah and C. Papadopoulos, "Characterizing International BGP Detours," Colorado State University, Tech. Rep. CS-15-104, 2015.

[63] "TeleGeography Submarine Cable Map," http://www.submarinecablemap.com/.

[64] N. Tyagi, Y. Gilad, M. Zaharia, and N. Zeldovich, "Stadium: A distributed metadata-private messaging system." *IACR Cryptology ePrint Archive*, vol. 2016, p. 943, 2016.

[65] J. Van Den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich, "Vuvuzela: Scalable private messaging resistant to traffic analysis," in *Proceedings of the 25th Symposium on Operating Systems Principles*. ACM, 2015, pp. 137–152.

[66] 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*. ACM, 2010, p. 15.

[67] 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*. Springer, 2012, pp. 200–210.

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

[69] X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, and D. G. Andersen, "Scion: Scalability, control, and isolation on next-generation networks," in *2011 IEEE Symposium on Security and Privacy*. IEEE, 2011, pp. 212–227.

[70] D. L. Zhihao Li, Stephen Herwig, "Detor: Provably avoiding geographic regions in tor," in *USENIX Security 2017*, 2017.

[71] S. Zhou, G.-Q. Zhang, and G.-Q. Zhang, "Chinese Internet AS-level topology," *Communications, IET*, vol. 1, no. 2, pp. 209–214, 2007.

APPENDIX A

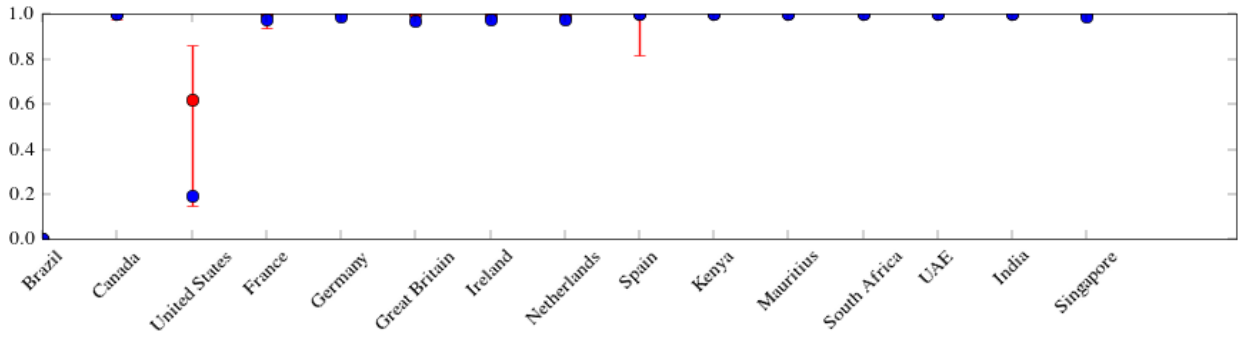


Figure 14: Avoidance plot for vantage point in Brazil. The lower limit bar represents the current fraction of paths that can avoid the country on the x axis, the blue dot represents the fraction of paths that can avoid the country using open DNS resolvers, the red dot represents the fraction of paths that can avoid the country using overlay network relays, and the upper limit bar represents the upper bound on avoidability for that country.

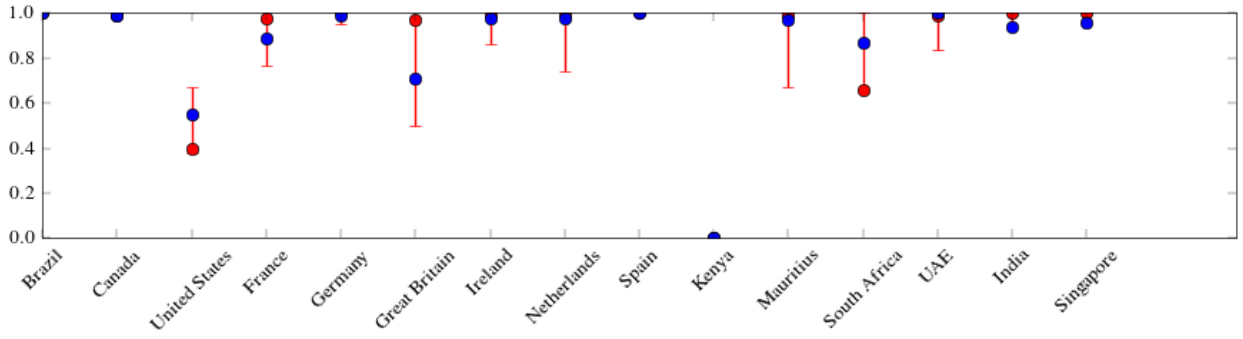


Figure 15: Avoidance plot for vantage point in Kenya. The lower limit bar represents the current fraction of paths that can avoid the country on the x axis, the blue dot represents the fraction of paths that can avoid the country using open DNS resolvers, the red dot represents the fraction of paths that can avoid the country using overlay network relays, and the upper limit bar represents the upper bound on avoidability for that country.