Analyzing G-20’s key autonomous systems and their intermeshing using AS-Analyzer

Sebastian Feld · Norbert Pohlmann · Michael Sparenberg · Bastian C. Wichmann

Institute for Internet Security – if(is)
Westphalian University of Applied Sciences Gelsenkirchen, Germany
{feld | pohlmann | sparenberg | wichmann}@internet-sicherheit.de

Abstract

Several thousands of interconnected autonomous systems form the Internet, which is regarded as the most powerful communication infrastructure today. Measuring the network and monitoring its vital parameters is crucial for securing continuous availability and steady performance of the Internet. This paper introduces AS-Analyzer, a tool for gathering and analyzing data related to autonomous systems and their interconnection. Using AS-Analyzer’s modules for collecting data from different sources, calculating key figures and creating reports, we present a vivid example by analyzing the G-20’s key autonomous systems and their intermeshing. A brief discussion of key figures related to autonomous system, IPv4 addresses, connections, categories and malware will complete the presentation.

1 Motivation

Given the fact that the Internet today is among the most critical parts of the global communication infrastructure [COMM09], the need arises to constantly monitor its vital conditions, measured by technical parameters regarding availability, performance, utilization and security. By analyzing and tracking these parameters using performance figure systems, we aim to provide data that improves the situational awareness of the net.

The Institute for Internet Security, a research facility of Westfälische Hochschule, Gelsenkirchen, develops and operates the Internet Key Figure System (IKS), a comprehensive database and tool set for internet-related information. Based on these key figures, the current state regarding security, performance and availability of the global network is constantly monitored and compared against historical average values to detect anomalies, short-term trends and long-term evolutions. This information is intended to be used by public and private stakeholders to identify potential risks, make necessary decisions in time and to check the effectiveness of actions taken. For more information in IKS, see [FPPS11a] and [FPPS11b].

The Internet as a whole consists of a fairly large amount (currently about 44,000) of separately managed networks, referred to as autonomous systems (AS), tied together by more than 400,000 interconnections. We are aware that the number of connections can never be measured correctly with reasonable effort and thus rather is a lower limit. On the one hand, a person or a tool does not notice every established connection between two AS and on the other hand, there are connections that are not publicly visible. Measuring the number and kind of connections of today's Internet, or the AS-level view on the Internet in general, is a well-known topic in research. Recently there are efforts to take into account the number of connections through public peering at Internet Exchanges Points, see [ACF+12] as an example.

It is essential to know about the role of each AS and possible implications when significant changes happen to the way how traffic is routed within the global infrastructure. Security incidents tend to grow in scale and scope and often result in extended downtime of popular websites (e.g. American Airlines, Paypal, Microsoft Update) or even whole countries, like the Libya take-down in late 2011[1].

Those incidents may have varying sources and reasons, from unintentional side effects of badly managed software roll-outs or malicious activities like denial-of-service attacks to secret military operations. But from a global perspective, they affect an increasing amount of users, slowing down business and resulting in loss of time and money[2]. Therefore, continuous availability of IP-based services is a high priority task. Extended budgets for public funded research projects reflect the increasing awareness and priority of Internet security among national governments and international institutions like the EC.

But beyond the short term perspective, it is essential to generate reliable, comprehensive data to estimate what is needed to meet future challenges. To achieve this goal, we designed a framework that comprises of tools and data to measure availability, performance, utilization and security of Internet traffic and services. This contribution illustrates a use case of this framework, analyzing the key autonomous systems of the G-20 and their intermeshing.

2 AS-Analyzer

The following section describes the key technical component used in this analysis. AS-Analyzer is a tool that aggregates information about autonomous systems from different data sources and generates key figures as well as rankings. There is a web frontend where the provided data is visualized in a convenient way. Furthermore there is a possibility to extract the key figures in form of tables, what is the base of our analysis in this contribution. The input data consists of information about BGP routing, IP address blocks, geolocation and malicious activities such as hosted malware.

2.1 Structure and Features

AS-Analyzer basically consists of a Java Enterprise backend and an Ext-GWT web frontend. The functionality can be divided into four parts.

Integration: AS-Analyzer uses many Internet data sources (see section 2.2) as input information. We implemented several parsers for the data sources to download, pre-process and integrate the information. These parsers are embedded into a software library.

Storage: AS-Analyzer’s backend is responsible for the long-term storage of the information determined and calculated as well for periodic updates.

Export: It is possible to export the information determined and calculated by AS-Analyzer into a comma separated value file. This file can be used to visually inspect the information, work with the results separately or integrate them in other applications such as spreadsheet applications.

Visualization: In order to visualize AS-Analyzer’s key figures, rankings and detailed AS-related information, we developed a web application using Ext-GWT.

[1] See, amongst others [HUFF11].

[2] See, amongst others [TECH11].

2.2 Data Sources

AS-Analyzer's architecture is very modular what simplifies the connection of new data sources. The current version of AS-Analyzer uses the following input:

- **Route Views**: We process the BGP routing tables [ROUT12] from Route Views, a project funded by the Advanced Network Technology Center at the University of Oregon.
- **RIPE RIS**: Routing Information Service (RIS) [RIPE12a] is a project from RIPE NCC, the Regional Internet Registry (RIR) responsible for Europe, the Middle East and parts of Central Asia. We extract routing information that amends the ones from project Route Views.
- **potaroo.net**: We determine the name for each autonomous system via a list [POTA12] offered by potaroo.net.
- **Regional Internet Registries**: We obtain more detailed information about an autonomous system via the corresponding RIR[3]. These include the number and size of allocated IP address blocks and the country of registration, amongst others.
- **Maxmind**: We use Maxmind's free APIs in order to perform IP address geolocation [MAXM12a] as well as mapping of IP addresses to autonomous systems [MAXM12b].
- **Google Safe Browsing**: Google's project Safe Browsing offers a "diagnostic page" [GOOG12] that gives an overview about the distribution of malware inside a given AS. The extracted information is described in the following section.
- **SiteVet**: Project SiteVet provides historical and current data on domains, IP addresses, AS numbers [SITE12a] and others across multiple blacklists. We extract security-related information explained in the next section.

2.3 Key Figures

The key figures measured and created by AS-Analyzer can be divided in four parts: Global, registry-related, country-related and AS-related information. Due to this contribution's focus on the G-20 countries we use the following arrangement: information related to autonomous systems, IPv4 addresses, connections, categories and malware.

AS-related information

These key figures make statements about the number of autonomous systems AS-Analyzer "sees" by means of the input data sources, e.g. BGP routing information. They can focus on the global number of AS, on the number of AS assigned to the G-20 and finally on each country separately. In this contribution we use the core definition of G-20 explained in section 3.1.

Furthermore we divide autonomous systems in branch AS and leaf AS. Branch AS are those AS-Analyzer found inside of routing paths, so they are necessary to reach certain other AS. Leaf AS appear just at the end of routing paths.

IPv4 address-related information

These key figures make statements about the number of IPv4 addresses advertised by autonomous systems "seen" by AS-Analyzer. Again, they can focus on the global number of IPv4 addresses, on the summed number of addresses the G-20 is responsible for and finally on the number of addresses of each country separately.

[3] For RIPE NCC, as an example, see [RIPE12b].

Furthermore AS-Analyzer makes statements about the average and median IPv4 addresses per autonomous system in a global context as well as in a country-related context.

Connection-related information

We sum up the connections seen by AS-Analyzer for each autonomous system by means of information extracted from BGP routing tables as well as whois information provided by project Routeviews or RIPE RIS. Since AS-Analyzer works on AS-level, we count every connection between two autonomous systems twice (from A to B and from B to A separately).

As with the key figures before, the context can be global, G-20 and country. We show the total number of connections as well as the average and medium number per autonomous system. This is an indicator for the global quality of AS intermeshing.

Category-related information

We use the heuristic explained in section 3.2 to assign autonomous systems to categories. An AS can have up to four categories: transit provider, content provider, access provider or business AS. There are statements about the absolute number of AS inside a certain category in the context of G-20 and the corresponding countries.

Malware-related information

These key figures give information about the penetration of malicious sites inside the autonomous systems of a country (core definition). They are separated into three values: The number of sites that causally lead to the infection of a user (category A), the number of sites that actually host malware (category B) and the number of sites that act as intermediaries (category C). For more information and a detailed definition see [PMAM08]. The values are taken from the diagnostic page of Google’s project Safe Browsing [GOOG12].

Furthermore AS-Analyzer crawled the so-called HostExploit Index and Rank from project SiteVet for each autonomous system. This is a calculated number that gives information about the “badness” of an AS. The HostExploit Index is a number between 0 and 1000, the higher the number, the more evil the autonomous system [SITE12b]. The HostExploit Rank is a sorted list of all existing autonomous system, number 1 being the worst [SITE12c].

The relevant numbers were averaged in order to compare the different G-20 countries.

3 A Detailed View on Global Infrastructure

From a technical point of view, it may seem questionable why anyone would want to break down a global network into small regional units. But when it comes to operational tasks like law enforcement, regulation and general responsibility, the physical location of infrastructure matters. AS-Analyzer is used to split up the whole set of autonomous systems by country, separating them by geo-localizing the IP addresses used by the respective system.

According to this policy, the geolocation of the majority of IPv4 addresses determines what country the AS belongs to. The resulting subset is referred to as “core autonomous systems” of Germany, for example. However, some applications require a broader definition that allows to include systems which are operating in Germany, for example, but primarily belong to another country.

3.1 Regional Mapping of AS

Core definition: The core set of a country's AS comprises of systems that have the majority of IPv4 addresses located there.

Extended definition: The extended set of a country's AS comprises of systems that have at least a minor share of IPv4 addresses located there.

3.2 Functional Categories of AS

Besides the extended and core definition for a nation-centric view on infrastructure we use a heuristic in order to categorize the analyzed AS. We define the four categories as followed:

- **Transit Provider**: AS has got ten or more potential transit customers (see the additional definition below).
- **Content Provider**: AS contains 75 or more hosted websites found by the Google Crawler. We use the value "visited websites" from Google's Safe Browsing's diagnostic page, since we crawl this and further information in order to make statements about the malware penetration inside the corresponding AS. For further information, see section 2.3.
- **Access Provider**: AS is responsible for more than 50,000 IPv4 addresses. We extract the number of addresses using the BGP information and the routed IP address blocks.
- **Business Customer**: AS that has got no potential transit customer by itself (see definition below) and is connected to less than four other autonomous systems.

The heuristic described above needs another one that makes a statement about the type of connections an autonomous system has got. In order to tell if an AS is a potential transit customer or provider we make the assumption that the AS-Analyzer's point of view – spoken with tier levels – is very low. That means we assume a top-down view from "big" providers to "small" customers. The definition is as followed:

- **Potential Transit Customers**: All AS that use the examined AS to reach other AS.
- **Potential Transit Providers**: All AS that route traffic for the examined AS.

In both cases the connected autonomous systems can also be peers on the same tier.

4 Discussion of AS-Analyzer's results

This chapter discusses an analysis of G-20's key autonomous systems and their intermeshing. The analysis has taken place on 6th and 7th of July 2012. AS-Analyzer's output can be divided into five parts: Key figures related to autonomous systems, IPv4 addresses, connections, categories and malware.

4.1 AS-related key figures

Table 1 shows, that AS-Analyzer recognized 44,061 different autonomous systems in our analysis. 6,525 of them were defined as branch AS (14.8%), since they can be found inside of routing paths. The other 37,536 AS are considered as leaf AS (85.2%), since they appear just at the end of routing paths.

Using our core definition to assign autonomous systems to G-20 countries, AS-Analyzer recognized 29,414 autonomous systems in our analysis to be in the G-20. That is, two-third of all AS seen (66.8%) can be assigned to G-20. The distribution of branch and leaf AS is very similar to the global view.

Table 1: Number of autonomous systems seen by AS-Analyzer divided in branch and leaf AS.

	Global	G-20	Non G-20
AS in total	44,061	66.8%	33.2%
Branch AS	6,525	63.3%	36.7%
Leaf AS	37,536	67.4%	32.6%

Figure 1 splits up the 29,414 autonomous systems assigned to G-20 to the respective countries. A G-20 country consists in average of 1,548 autonomous systems. The biggest country by the total number of AS is the United States with 14,614 AS, followed by Russia with 4,167 AS. The United Kingdom (1,435 AS), Germany (1,385 AS) and Brazil (1,290 AS) are very near the average. China, an interesting country as we will see later, consists of just 224 AS.

Compared to the G-20, the United States represents 49.7% and Russia 14.2% of G-20's AS.

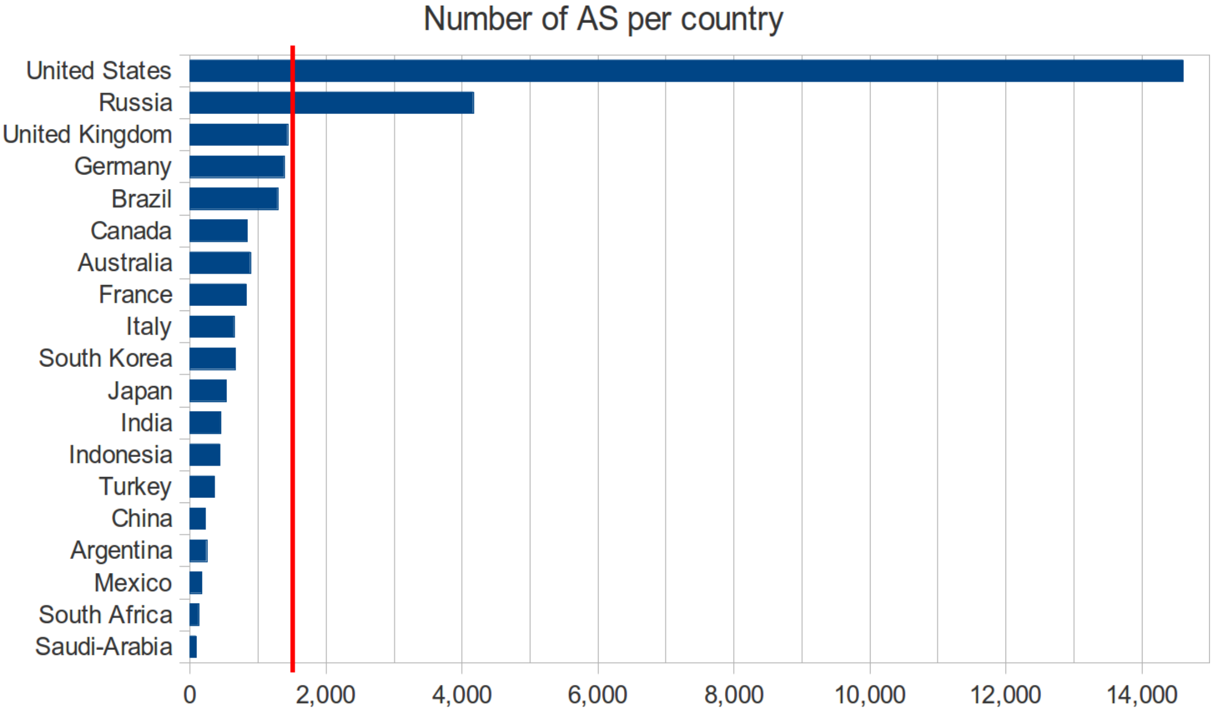


Fig. 1: Number of autonomous systems (core definition) per G-20 country.

4.2 IPv4 address-related key figures

The IPv4 address space contains about 4.3 billion addresses. When we subtract the nearly 662 million IPv4 addresses reserved for special purposes (e.g. for private use) we get roughly 3.7 billion usable IPv4 addresses. In our analysis AS-Analyzer saw about 2.56 billion advertised IPv4 addresses. This is about 69.8% of the usable IPv4 addresses (see Table 2). This underlines the exhaustion of the IPv4 address space and justifies the ongoing adoption of IPv6.

Utilizing our categorization to group autonomous systems into G-20 AS and others, the G-20 consists of about 2.1 billion IPv4 addresses and thus represents 82% of the advertised and 57% of the overall usable IPv4 addresses.

Table 2: Comparison of IPv4 address space, usable and advertised addresses.

	IPv4 addresses
IPv4 address space	4,294,967,296
IPv4 addresses for special purpose[4]	622,199,809
Usable IPv4 addresses	3,672,767,487
Advertised IPv4 addresses	2,563,368,745
Advertised IPv4 addresses assigned to G-20	2,102,625,791

Table 3 shows, that on average an autonomous system is responsible for 58,177 IPv4 addresses. The median is 1,024 IPv4 addresses per AS.

Table 3: Average and median IPv4 addresses per autonomous system.

	IPv4 addresses	**Comment**
Average IPv4 addresses per AS	58,177	near /16 network size
Median IPv4 addresses per AS	1,024	equals /22 network size

Figure 2 illustrates the total number of advertised IPv4 addresses seen by AS-Analyzer grouped by G-20 countries. The average G-20 country is responsible for roughly 110 million IPv4 addresses. The country with the most IPv4 addresses is the United States, holding about 47% of G-20's advertised IPv4 addresses. Far beyond, China is on place two by holding about 13% of G-20's advertised IPv4 addresses. This is quite interesting, since Figure 1 showed that China is responsible for just 224 AS. For comparison, the United States consists of more than 14,000 AS. The next figure will show the ratio "IPv4 addresses per AS" in detail.

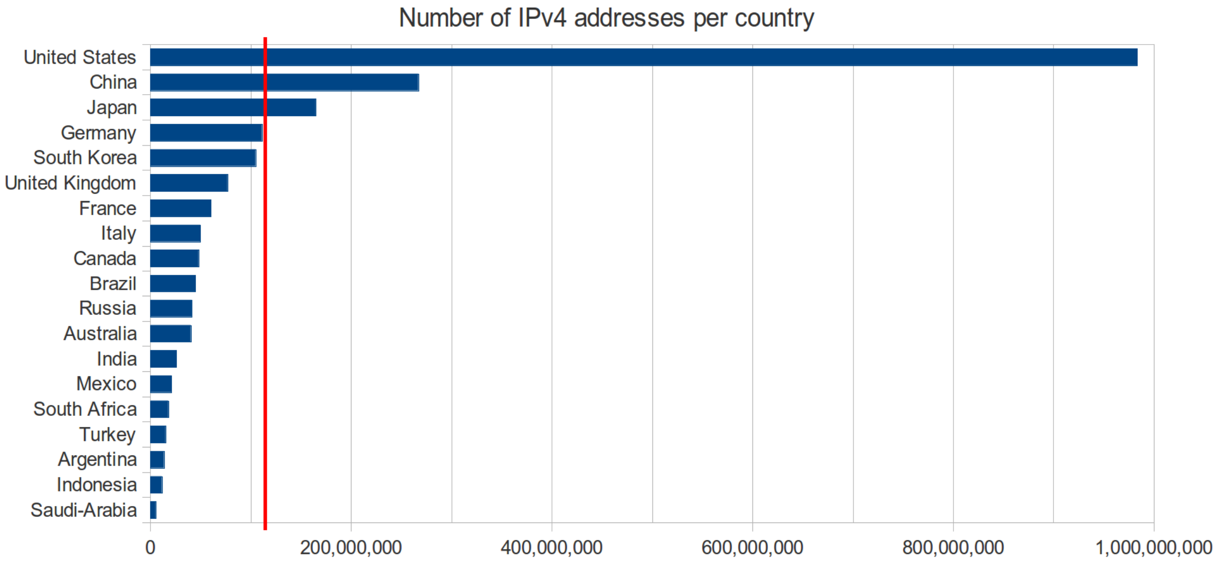


Fig. 2: Total number of IPv4 addresses per G-20 country.

Figure 3 shows the average number of IPv4 addresses per autonomous system for each G-20 country. One can see easily, that every country except China and Japan has less than 160,000

[4] Value is calculated via RFC1918, RFC2544, RFC3068, RFC3171, RFC3232, RFC3330, RFC3927, RFC5737 and RFC6598.

IPv4 addresses per autonomous system. In fact, the G-20 average for IPv4 addresses per AS is about 140,000. The enormous value of about 1.2 million IPv4 addresses per AS for China results from the few number of 224 AS assigned to that country, like mentioned before.

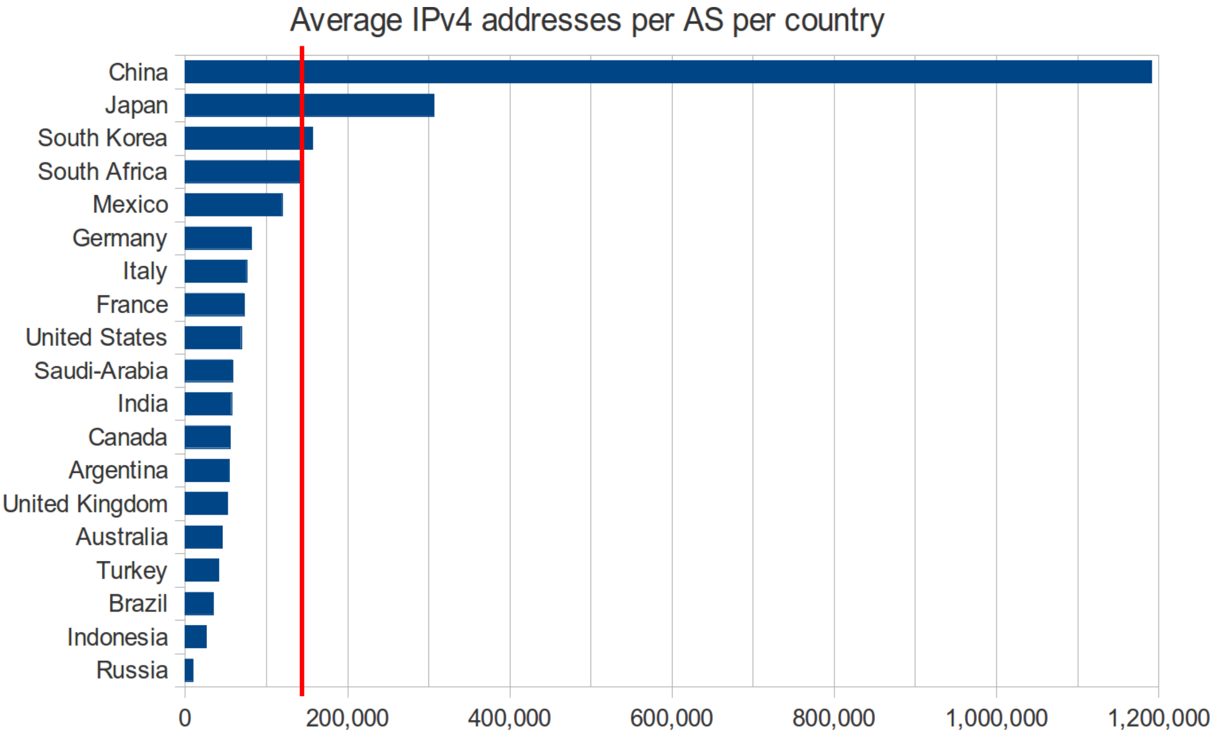


Fig. 3: Average IPv4 addresses per autonomous system for each G-20 country.

4.3 Connection-related key figures

As mentioned before, we count every connection between two autonomous systems twice (from A to B and from B to A separately). In our analysis AS-Analyzer identified about 400,000 connections with an average of 9.06 connections per autonomous system, see Table 4. When using our definition of the G-20 autonomous systems, the connections to or from G-20 AS compose about 64% of all connections. The average connection per AS is slightly lower in the G-20 compared to the global view.

Table 4: Number of connections seen by AS-Analyzer.

	Global	**G-20**	**Non G-20**
Number of connections	399,056	64.2%	35.8%
Average connections per AS	9.06	8.72	9.74
Median connections per AS	2	2	2

Figure 4 visualizes the roughly 256,000 connections from or to AS in G-20 countries seen by AS-Analyzer and groups them by country. The average number of connections per country is about 13,500. The country with the biggest total number of connections is the United States with about 78,000 connections. Thus, the United States is responsible for roughly 30.4% of G-20's AS connections. The following countries are Russia with about 43,000 connections and a share of roughly 17%, United Kingdom (approx. 42,000 connections, about 16% of G-20's connections) and Germany (approx. 37,000 connections, 14% share). This numbers strongly correlate to the absolute number of autonomous systems assigned to a country, see Figure 1.

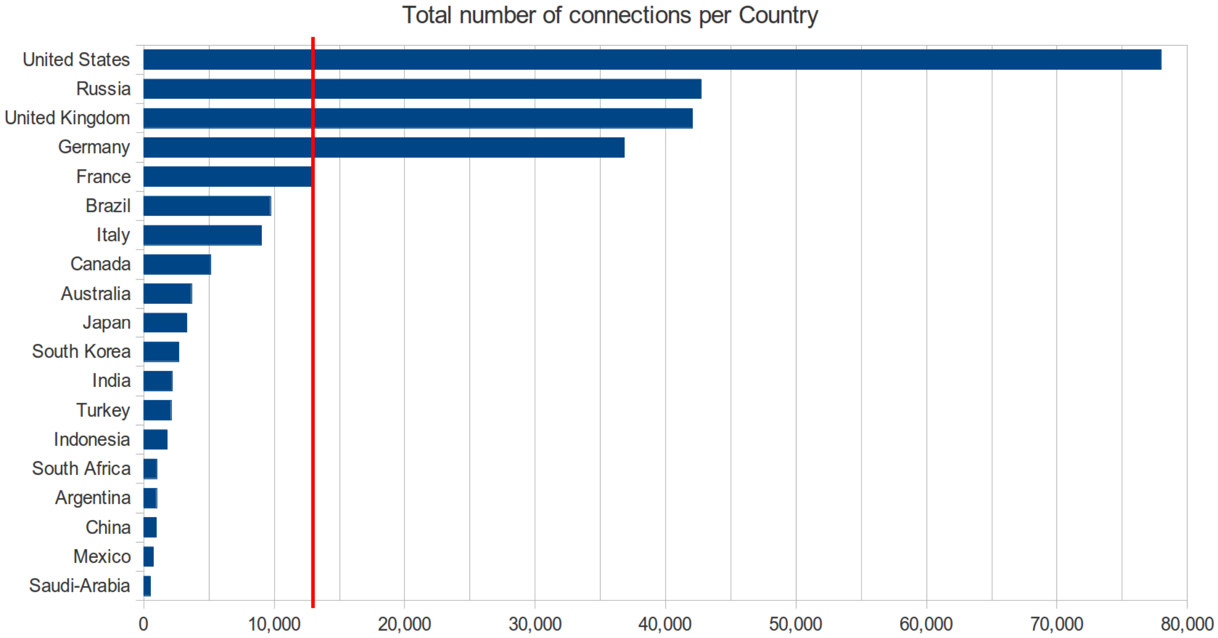


Fig. 4: Total number of connections per G-20 country.

Figure 5 also shows the number of connections per country, but averaged by the number of corresponding AS. One can see that an average G-20 country has about 9 connections per AS. United Kingdom has got 29 connections per autonomous system in average, followed by Germany with 27 connections, France (16), Italy (14) and Russia (10).

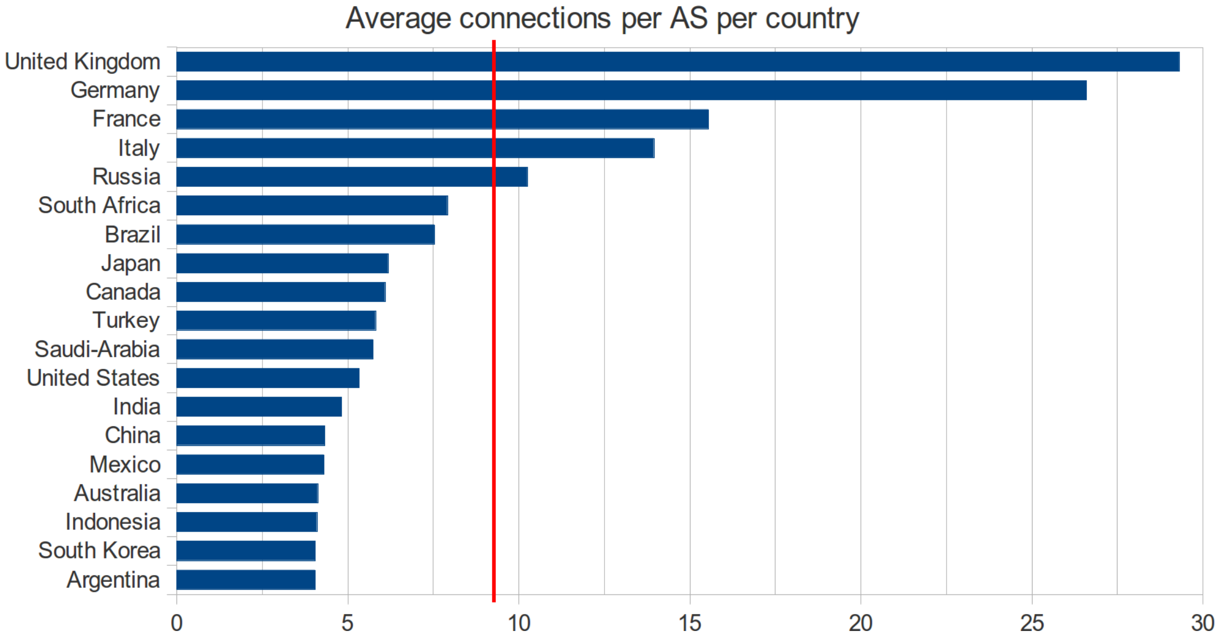


Fig. 5: Average connections per autonomous system for each G-20 country.

4.4 Category-related key figures

Table 5 shows the number of autonomous systems AS-Analyzer assigned to the four categories defined in section 3.2. As you can see, most of the autonomous systems (about 74%) were grouped into the category business AS.

Table 5: Distribution of the categories assigned to the AS of G-20 seen by AS-Analyzer.

	Number of AS (G-20)	**Share**
Transit Provider	1,648	5.60%
Access Provider	2,995	10.18%
Content Provider	2,800	9.52%
Business AS	21,862	74.33%
Total	29,414	-
Note: Multiple categories (and even none) can be assigned to a single AS.		

Figure 6 visualizes the number of AS in each category by country. Please note that the figure is cropped at 2,500 AS, resulting in a truncated bar of business AS in the United States.

Referring to the countries containing the most business AS, United States is on the first place with 12,047 AS, followed by Russia with 2,425 AS and United Kingdom (820 AS). When comparing the total number of access provider, the United States is on place 1 with 1,721 AS, followed by Japan (173 AS) and Russia (139 AS). After applying the heuristic for categorizing the AS and sorting by total number of transit providers, first place is held by Russia with 425 AS, United States (317 AS) and United Kingdom (256 AS). The last category is content provider with United States (1,202 AS), Germany (247 AS) and United Kingdom (226 AS).

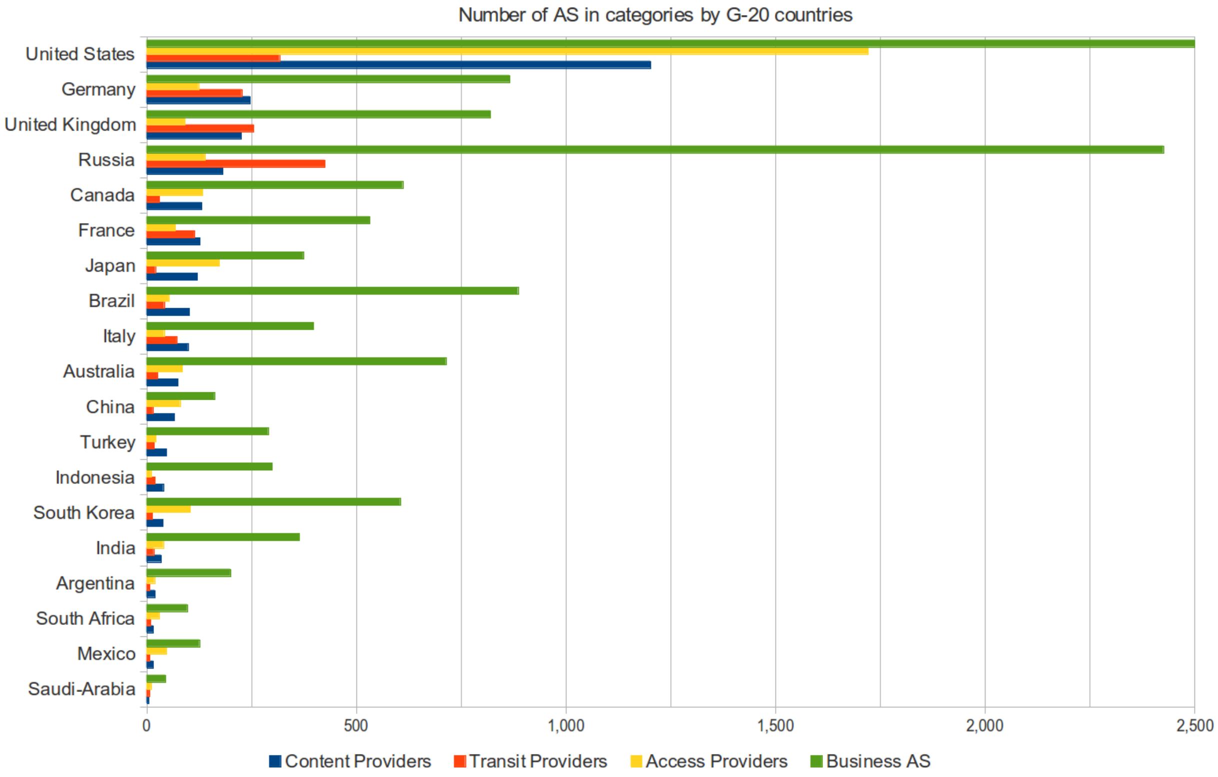


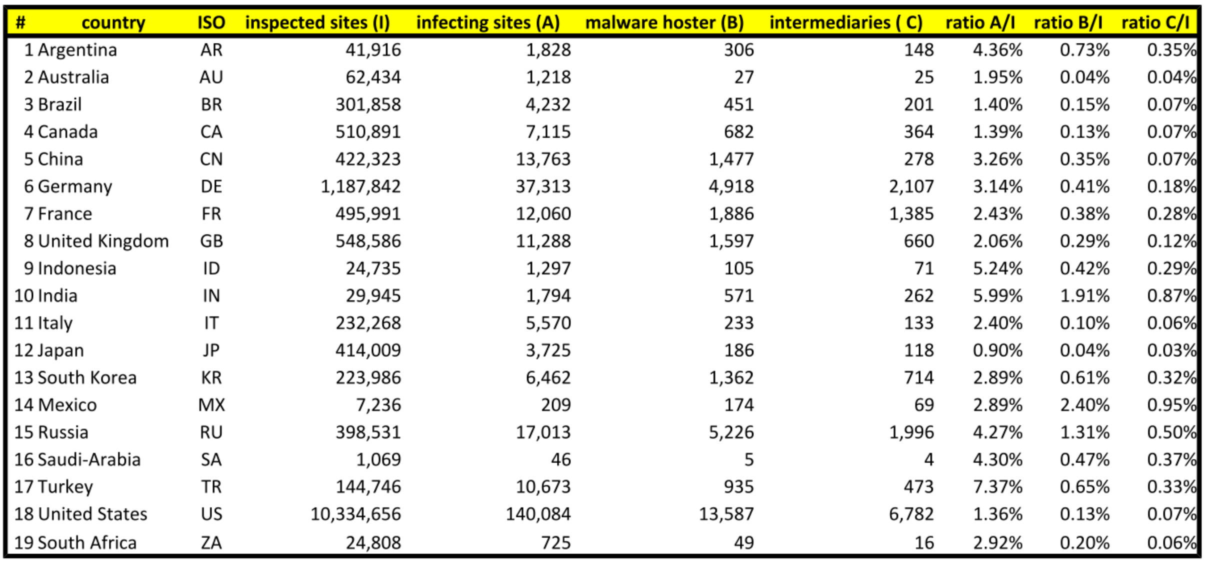
Fig. 6: Number of AS grouped by the categories transit provider, access provider, content provider and business AS for each G-20 country. Note: The figure is truncated at 2,500 AS.

4.5 Malware-related key figures

Figure 7 summarizes the amount and type of malicious software samples found inside a country's autonomous systems. Ratio values show the percentage of actually infected websites from the set of sites selected for inspection by Google Safe Browsing.

The table shows that in Turkey, India and Indonesia more than 5% of all inspected websites serve content that results in malicious software being downloaded and installed without user consent. On the opposite side, Japan has a share of malware sites below 1 per 100, followed by the US, Canada, Brazil and Australia, which all successfully manage to keep their malware ratio below the level of 2%. The number of sites acting as intermediaries for spreading malware is distributed more evenly among the G-20, varying roughly between 1% (Mexico) and 0.03% (Japan).

The statistics of malware hosting network sites is led by Mexico and India, which have a share of 2.4 and 2.0 percent of websites with physically hosted malicious software. Australia and Japan are the most secure countries according to this category, where less than one per twenty systems are infected.



#	country	ISO	inspected sites (I)	infecting sites (A)	malware hoster (B)	intermediaries (C)	ratio A/I	ratio B/I	ratio C/I
1	Argentina	AR	41,916	1,828	306	148	4.36%	0.73%	0.35%
2	Australia	AU	62,434	1,218	27	25	1.95%	0.04%	0.04%
3	Brazil	BR	301,858	4,232	451	201	1.40%	0.15%	0.07%
4	Canada	CA	510,891	7,115	682	364	1.39%	0.13%	0.07%
5	China	CN	422,323	13,763	1,477	278	3.26%	0.35%	0.07%
6	Germany	DE	1,187,842	37,313	4,918	2,107	3.14%	0.41%	0.18%
7	France	FR	495,991	12,060	1,886	1,385	2.43%	0.38%	0.28%
8	United Kingdom	GB	548,586	11,288	1,597	660	2.06%	0.29%	0.12%
9	Indonesia	ID	24,735	1,297	105	71	5.24%	0.42%	0.29%
10	India	IN	29,945	1,794	571	262	5.99%	1.91%	0.87%
11	Italy	IT	232,268	5,570	233	133	2.40%	0.10%	0.06%
12	Japan	JP	414,009	3,725	186	118	0.90%	0.04%	0.03%
13	South Korea	KR	223,986	6,462	1,362	714	2.89%	0.61%	0.32%
14	Mexico	MX	7,236	209	174	69	2.89%	2.40%	0.95%
15	Russia	RU	398,531	17,013	5,226	1,996	4.27%	1.31%	0.50%
16	Saudi-Arabia	SA	1,069	46	5	4	4.30%	0.47%	0.37%
17	Turkey	TR	144,746	10,673	935	473	7.37%	0.65%	0.33%
18	United States	US	10,334,656	140,084	13,587	6,782	1.36%	0.13%	0.07%
19	South Africa	ZA	24,808	725	49	16	2.92%	0.20%	0.06%

Fig. 7: Summary after crawling Google's Project Safe Browsing.

The scatter chart in Figure 8 gives a visual representation of the distribution of AS-specific HostExploit Ranking values per country. While the majority of G-20 states have their rankings distributed evenly over the whole range, some countries like Indonesia and Turkey show a lack of top-rated AS, meaning that none of their autonomous systems belong to the group of highly secure systems.

Despite the fact that the amount and size of AS per country varies greatly and thus many key values may not be comparable, the figure points out to some important statistical characteristics regarding the ranking. Most evidently is a gap in the mid-range position with HostExploit Index values between about 12,000 and 20,000, which means that these ranking positions will be more typical outside the G-20.

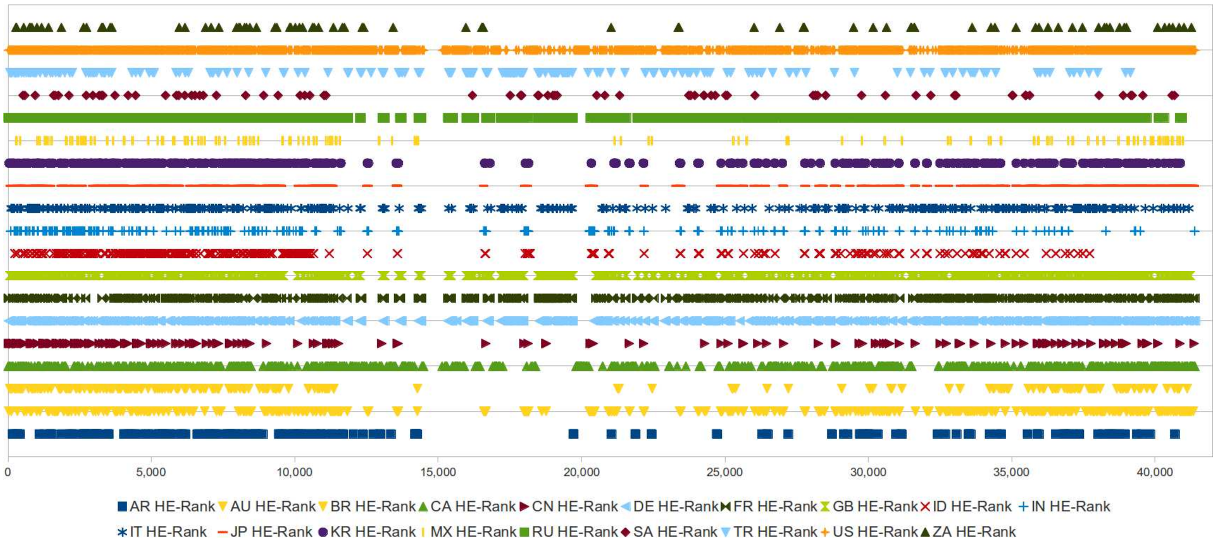


Fig. 8: Spread of HostExploit Index values by G-20 country.

According to the heuristics described in chapter 3.2, Figure 9 illustrates the average Host Exploit Index per category (Content / Transit / Access / Business) of a country’s autonomous systems within the G-20. It shows what kind of systems contribute most to the whole amount of malware found on their national AS.

Most countries indicate an asymmetric distribution pattern, where transit providers serve the largest amount of malware to the client, followed by decreasing shares of content and access providers and a minor share of business AS.

UK, France and Germany are exceptions worth mentioning, since they show a rather evenly distributed set of infected websites among content and transit providers. Summing up the values for each category, China and India claim the top positions of the ranking with the highest level of infections measured by a combination of all categories.

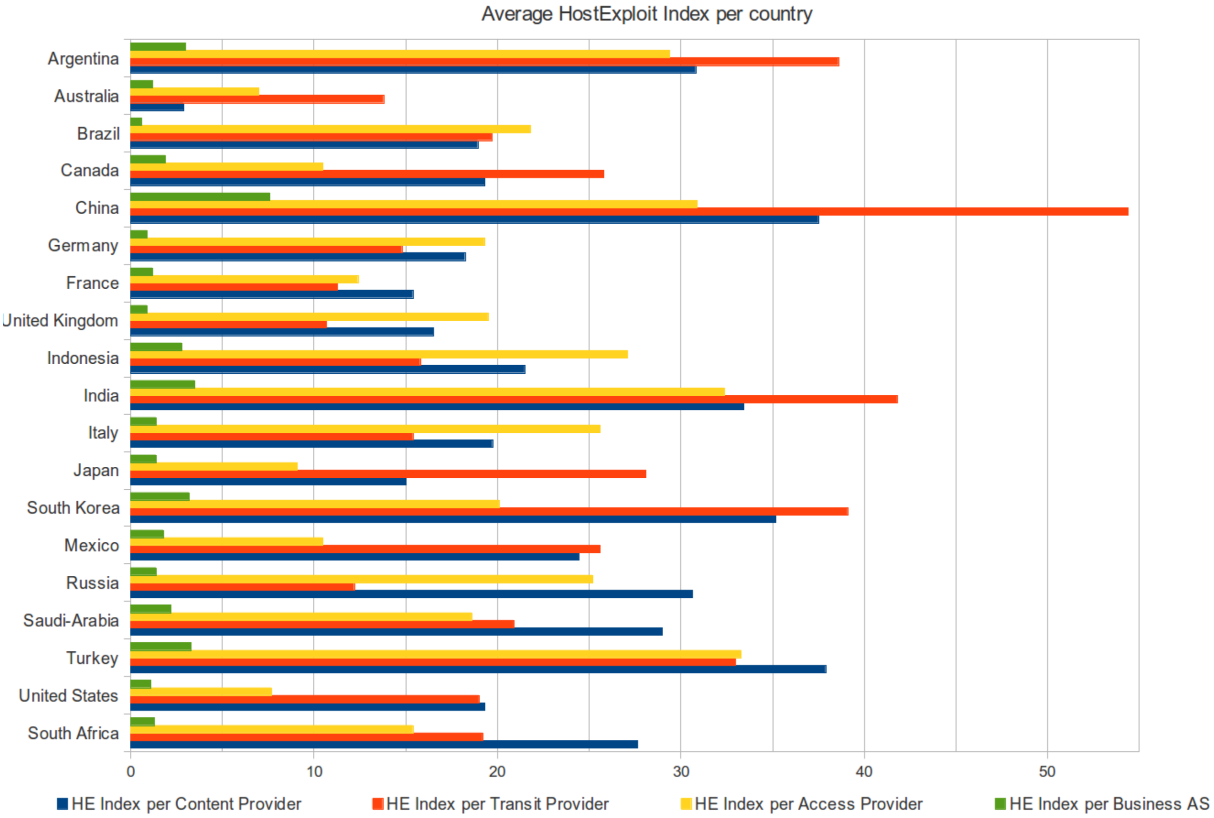


Fig. 9: Average HostExploit Index per category and country.

5 Conclusion

According to AS-Analyzer the today's global Internet consists of nearly 44,000 autonomous systems with more than 399,000 connections. That means that there are in average 9.06 connections per AS. After assigning AS to countries and thus getting a "G-20 Internet", almost two-thirds of the global AS belong to the G-20 countries. This ratio counts for the connections as well. A remarkable G-20 country is China, responsible for about 13% of G-20's advertised IPv4 addresses with just 224 autonomous systems. This fact results in a ratio of 1.2 million IPv4 addresses per AS for China, while the G-20 average is about 140,000.

Regarding the spread of malware, it is important to keep in mind that several hot spots of malicious network activities are outside the scope of G-20 and thus will not show up in the corresponding statistics. This selection has been made intentionally and is not a technical limitation of AS-Analyzer, since all key figures may have a global or local scope, depending on the measurement setup.

One essential result of validating AS-Analyzer's findings is that the overall quality of output - especially the precision of statistical key figures generated - heavily depends on the quality of input data in terms of validity and completeness. Given the fact that net routing measurements may only be conducted over parts of the global infrastructure, the resulting picture of intermeshing can never be perfect. On the other hand, a carefully chosen measurement setup ensures the highest level of quality possible regarding the input. Some result may require non-technical context information to be properly interpreted, e.g. the ratio of IP addresses per AS found in China. Others will show an extraordinary volatility, making it difficult to draw conclusions from a limited set of values.

The given example shows how Internet key figures can be automatically generated by AS-Analyzer. The resulting data set provides a comprehensive snapshot of essential parameters describing the current state of the global network. Continuous measurements (conducted on a regular basis) will extend the usefulness of this tool in future use, adding historical data and statistical values to a long-term database that allows a distinction of regular patterns and technical anomalies. Furthermore, IPv6 will be integrated into AS-Analyzer's data gathering modules, allowing to detect future changes in the utilization of transport protocols and security related improvements of net traffic. It is planned to release AS-Analyzer's web user interface as a plugin of an Internet accessible web application, the Internet Key figure System (IKS), extending its usefulness and making it available to the general public.

Acknowledgment

This work is part of the project "Deutscher Internet-Index (DIX)"[5], which is funded by the Federal Ministry of Economics and Technology (BMWi). The contents of this publication is solely in charge of the authors and reflect in no way the BMWi's opinion.

References

[ACF+12] Ager, Bernhard; Chatzis, Nikolaos; Feldmann, Anja; Sarrar, Nadi; Uhlig, Steve; Willinger, Walter: Anatomy of a Large European IXP. In: ACM SIGCOMM '12. 2012.

[COMM09] Commission of the European Communities: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. 2009.

[FPPS11a] Feld, Sebastian; Perrei, Tim; Pohlmann, Norbert; Schupp, Matthias: Objectives and added value of an Internet Key Figure System for Germany. In: ISSE 2011 Securing Electronic Business Processes. Vieweg+Teubner Verlag, 2011.

[FPPS11b] Feld, Sebastian; Perrei, Tim; Pohlmann, Norbert; Schupp, Matthias: Ein Internet-Kennzahlensystem für Deutschland: Anforderungen und technische Maßnahmen. In: D-A-CH Security 2011. IT-Quartier Oldenburg, 2011.

[GOOG12] Google.com: Google Safe Browsing diagnostic page for AS680 (DFN). http://www.google.com/safebrowsing/diagnostic?site=AS:680. Last access: 16.07.2012.

[HUFF11] The Huffington Post: Libya's Internet goes down. http://www.huffingtonpost.com/2011/03/04/libya-internet-down_n_831506.html. Last access: 16.06.12.

[MAXM12a] Maxmind.com. http://www.maxmind.com/download/geoip/database/GeoLiteCountry/GeoIP.dat.gz. Last access: 16.07.2012.

[MAXM12b] Maxmind.com. http://www.maxmind.com/download/geoip/database/asnum/GeoIPASNum.dat.gz. Last access: 16.07.2012.

[5] German for "German Internet Index".

[PMAM08] Provos, Niels; Mavrommatis, Panayiotis; Abu Rajab, Moheeb; Monrose, Fabian: All Your iFRAMEs Point To Us. Google Technical Report. 2008.

[POTA12] potaroo.net. http://bgp.potaroo.net/cidr/autnums.html. Last access: 16.07.2012.

[RIPE12a] RIPE NCC: Routing Information Service (RIS) - RIPE Network Coordination Centre. http://www.ripe.net/data-tools/stats/ris/routing-information-service. Last access: 16.07.2012.

[RIPE12b] RIPE NCC. ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest. Last access: 16.07.2012.

[ROUT12] Routeviews.org. http://archive.routeviews.org/oix-route-views/. Last access: 16.07.2012.

[SITE12a] Sitevet.com: SiteVet Autonomous System Report AS680 - DFN. http://sitevet.com/pdf/asn/AS680. Last access: 16.07.2012.

[SITE12b] Sitevet.com: HE Index. http://sitevet.com/info/he_index.php. Last access: 16.07.2012.

[SITE12c] Sitevet.com: HE Rank. http://sitevet.com/info/he_rank.php. Last access: 16.07.2012.

[TECH11] Technorati: Egypt Counts Cost of Protests, Internet Down-Time. http://technorati.com/politics/article/egypt-counts-cost-of-protests-internet/. Last access: 16.07.2012.

Index

Internet Measurement, Critical Infrastructure, Autonomous Systems, Key Figures, G-20