Network-Political Resiliency

A Classification of Internet Resiliency by Country

Chloe Reynolds & Saghar Tamaddon

Abstract

Recent Internet disruptions in Libya, Egypt, Syria, Burma and Nepal beg the question, "How vulnerable is any country to an Internet access disruption by its government?" This paper seeks to answer that question by taking a look at both internet infrastructure and politics to create a 'Network-Political Resiliency' (NPR) classification. The network infrastructure metric for each country is based on Roberts and Larochelle's (2010) number of 'Points of Control' (POCs). POCs are the most influential Autonomous Systems (ASs) in a country's Internet network. Roberts and Larochelle determined the POCs based on a new AS relationship inference method, applied to data from The Cooperative Association for Internet Data Analysis (CAIDA). Three different political metrics are used, gathered from two sources: a) OpenNet Initiative's Political Internet Filtering score (see map in Appendix 2), b) OpenNet Initiative's overall Internet Filtering score, and c) Reporters Without Borders' Internet Enemies Report (see map in Appendix 3). The combination of these metrics results in a final NPR classification. In short, only a small portion of countries has a "high" NPR classification, and most fall into the low and very low resiliency categories. Given that Internet access is felt by many to be a matter of human rights, national NPR levels can be a red flag for concerned entities, such as human rights organizations. NPR ratings can also serve as a call for increasing network infrastructure.

Political Infrastructure of the Internet

Proponents of open Internet access and net neutrality argue that unfiltered widely and freely available Internet access is a democratization tool (Reporters Without Borders, 2011). Many note that the Internet has become a battleground between the government and its citizens (Roberts and Larochelle, 2010, Deibert et al. 2008, Faris et al., 2008, OpenNet Initiative, 2011, Reporters Without Borders, 2011). Many governments have attempted to control Internet usage or Internet contents (OpenNet, 2011, Warf, 2011). "Certain regimes sometimes intentionally keep their infrastructural problems to prevent their populations from having Internet access" (Reporters Without Borders, 2011). North Korea only just launched its own online social networks in 2010; an official policy of making internet use illegal predated this move. As of March 2011, 119 netizens (Internet citizens) were imprisoned and imprisoned netizens have been sentenced to death in Iran for the first time (Reporters Without Borders, 2011).

Network Infrastructure of the Internet

Autonomous systems, points of control and resiliency are defined in order to then discuss the internet infrastructure metric used in NPR classifications. An Autonomous System (AS), or network domain, is a collection of IP networks and routers, usually under the control of a single administrative entity that presents a common routing policy to the Internet. Examples of ASs are ISPs, corporations and universities (Chuang, 2011).

Roberts and Larochelle summarized that "even though the Internet is theoretically structured as a random game of hot potato with no particular autonomous system serving as the center of the network, in practice a very small portion of those autonomous systems carry the traffic for a disproportionate number of routes on the Internet (Huffaker and Claffy 2009)" (2010). About 30,000 ASs exist worldwide. They deliver traffic to billions of IP addresses. Yet, Roberts and Larochelle identified only 579 of these 30,000 ASs as "Points of Control." They go on to explain:

> "Data flowing from a computer in China to a computer in the U.S. will likely travel through one of a handful of Chinese autonomous systems connecting China to the rest of the world and one of a few U.S. autonomous systems connecting the U.S. to the rest of the world. This concentration of traffic on only a few autonomous systems per country further amplifies the technical /political role of those autonomous systems and their resulting role as the loci of national control over the Internet. The key finding of this paper is that this concentration of autonomous systems holds within individual countries as well as for the Internet as a whole. In any country, a much smaller subset of all of the country's autonomous systems act as a chokepoint for control of the larger set of autonomous systems and for the much larger set of people using the network" (2010).

Internet resiliency means that if one or more component is removed, the remaining parts of the Internet should be able to continue working (Chuang, 2011). The NPR level introduced in this paper considers the resiliency of Internet access in this sense, since it accounts for the removal of POC's. In addition, however, it also takes into account a government's position on Internet freedom, which can either compound or relieve the network resiliency.

The interplay of political and network internet infrastructures

In this paper, the strength of a country's network infrastructure (its resilience) and its government's political approach to Internet control together yield a metric called NPR (Network-Political Resiliency).

Zittrain and Palfrey enumerate five ways to control the Internet. One is through placing liability on the ISPs (ASs) and Internet Service Content Providers. Other ways are with content restrictions, licensing requirements, Internet filtering and surveillance (2008). Since Internet access can be thwarted at any of these stages of communication, it is important to recognize that the political part of NPR classifications only encompass four of these five methods. The censorship ratings of OpenNet Iniative and Reporters Without Borders address the latter four methods. The first internet control method is not incorporated into the NPR, due to lack of easily locatable data on this internet control feature.

When either network infrastructure or political infrastructure is considered alone, a misleading picture can develop. Whether national censorship structures might affect the number of ASs or vice versa or both, or neither, the intersection of the two paints a more complete picture.

Interest in Resilience

Several researchers have expressed interest in the resilience of network infrastructures, including the authors of the parent and grandparent papers on which this paper is based. Dimitropoulos et al. (2007) define the driving force behind their AS inference work: "The relationships among ASs in the Internet represent the outcome of policy decisions governed by technical and business factors of the global Internet economy. Precise knowledge of these relationships is therefore an essential building block needed for any reliable and effective analysis of technical and economic aspects of the global Internet, its structure, and its growth." Roberts and Larochelle were also aware of political use of the Internet: "We have found no evidence that [Roberts and Larochelle's metrics, including Points of Control] for national Internet control directly predict whether a country exerts specific kinds of control over its Internet – for instance by filtering content. But they may provide a map for understanding better both how the countries exert control over their networks and how philosophies of political control in the countries have shaped the technical details of their local portions of the Internet" (2010).

Network Infrastructure Prior Work

This paper adds to the work of Roberts and Larochelle (2010). Roberts and Larochelle based their research on the earlier findings of Dimitropoulos et al. (2007). The goal of Dimitropoulos at CAIDA and his colleagues was to infer contractual relationships between ASs. They improved upon existing inference methods in a number of technical ways. (For a complete discussion, see Dimitropoulos et al. 2007.) For example, one prior method of inferring ASs was from Border Gateway Protocol (BGP) tables. However, using BGP tables to infer AS relationships misses 86% of actual relationships, whereas Dimitropoulos et al.'s approach captured 94% of relationships. (Both percentages are in comparison to the 3,724 known

relationships derived from an AS owner survey which will be explained momentarily.) Furthermore, after computing AS relationships using their inference technique, Dimitropoulos et al. attempted to validate their data by directly communicating with AS owners to verify that the inferred relationships were indeed correct. This survey yielded 3,724 data on AS relationships from 38 AS owners (including 5 tier-1 ISPs). The percent of correctly inferred relationships was highly accurate (94.2% for overall relationships, 96.5% of c2p, 82.8% of p2p, and 90.3% of s2s relationships) (Dimitropoulos et al., 2007). One limit of the data is the percentage, albeit a small percentage, of inaccurately inferred relationships. Dimitropoulos et al. note too that their survey was subject to sampling bias. Also, the 3,724 ASs that were confirmed represent only 9.7% of the total number of links in their data (2007).

Roberts and Larochelle built upon the CAIDA data in their study, "Mapping Local Internet Control." Curious about national governments' ability to control the Internet, Roberts and Larochelle computed a metric called a "Point of Control," among other computations. A Point of Control is 1 of n ASs in a country that would need to be shut down in order for 90% of a country's IP addresses to be disconnected from the internet (2010). For example, while China has 192 ASs, it only has 4 Points of Control. This means the Chinese government would only need to shut down 4 ASs to interrupt internet service to 90% of Chinese IP addresses.

Network-Political Resiliency (NPR)

Inspired by Roberts and Larochelle's comment that number of ASs has no evidence as a predictor of Internet Filtering (2010), I had a similar question. I found two entities that investigate a country's level of Internet censorship. The first entity is OpenNet Initiative's Political Filtering score (provided by OpenNet Initiative) and Overall Filtering score (calculated by author, based on four separate OpenNet Initiative scores). The second is Reporters Without

Borders' 2011 'Enemies of the Internet' report. The four OpenNet Initiative scores are 1) "Political content: Content that expresses views in opposition to those of the current government, or is related to human rights, freedom of expression, minority rights, and religious movements"; 2) "Social content: Content related to sexuality, gambling, and illegal drugs and alcohol, as well as other topics that may be socially sensitive or perceived as offensive"; 3) "Conflict & security: Content related to armed conflicts, border disputes, separatist movements, and militant groups"; and 4) "Internet tools: Web sites that provide e-mail, Internet hosting, search, translation, Voice over Internet Protocol (VoIP) telephone service, and circumvention methods" (OpenNet, 2011). Reporters Without Borders makes its determination of which countries are labeled Internet Enemies or Countries Under Surveillance based on various forms of online censorship, such as arrests or harassment of netizens, online surveillance, website blocking or the adoption of repressive Internet laws (Reporters Without Borders, 2011).

This project categorizes countries based on Network-Political Resiliency (NPR). NPR combines one network infrastructure metric and three political Internet infrastructure metrics. Network infrastructure was operationalized as a country's POC Redundancy Level. I derived the POC Redundancy Level from Roberts and Larochelle's (2010) number of POCs. A country with over 50 POC's yielded a 'High" POC Redundancy Level rating; between 13 and 50 was 'Moderate'; between 7 and 12 was 'Low"; and 6 or fewer POCs received a 'Very Low' POC Redundancy Level rating. The cut-off points between each POC Redundancy level were based on my subjective opinion of the numbers of POC's that could be controlled by a government more or less easily. The three political metrics, on the other hand, were used in their original forms in the final NPR rating computation. These were

The specific algorithm used to classify each country as 'High', 'Moderate', 'Low', or 'Very Low' in NPR is below.

To have a Very Low NPR classification any of these three conditions must exist:

- Political Filtering: 3 or 4
- Total Filtering: 12 or higher
- Internet Enemies: on list (as 'Countries under surveillance' or as 'Internet Enemies')

To have a Low NPR classification either of these sets of conditions must exist:

- Country is not rated Very Low already;
  - and POC Redundancy Level: Very Low
- Country is not rated Very Low already;
  - and Political Filtering: 2 or less
  - and Total Filtering: 8 or less
  - and POC Redundancy Level: Low

To have a Moderate NPR classification this set of conditions must exist:

- Country is not already rated Low or Very Low;
  - and Political Filtering: 0
  - and Total Filtering: 4 or less
  - and POC Redundancy Level: Moderate

To have a High NPR classification this set of conditions must exist:

- Country is not already rated Moderate, Low or Very Low;
  - and Political Filtering: 0
  - and Total Filtering: 4 or less
  - and POC Redundancy Level: High

Results

The map below visualizes the NPR classification results. Darker green indicates higher NPR. Appendix 1 shows the same information in a list format.

Of the 152 countries rated, only one country, the United Kingdom, was classified as High NPR. Nineteen countries were classified as Moderate NPR, while the 101 fell into the Low NPR classification and 31 into the Very Low NPR classification.

This is not surprising. For perspective, the entire Internet itself was found vulnerable to deliberate attacks. Reachability drops over 50% with removal of the 25 most connected nodes and the Internet disintegrates much faster than previously found if the top .5% of ASs [i.e. the top POCs] are targeted (Dolev et al., 2006). Therefore, finding only 20 countries - of the 152 evaluated countries – to have High or Moderate NPR classifications was not surprising. This finding, however, does mean that creating incentives to moderate political control and/or increase infrastructure survivability is an important aim for entities who value NPR.

Limitations of NPR Classification

Internet Network Resiliency can be measured in many ways. Political Internet control can be as well. I operationalized network infrastructure survivability through the number of POCs. Selecting different network infrastructure parameters might have yielded different NPR rating for some countries.

This study measured this ability of a government to control its own resident's internet access. Another study could evaluate the connectivity dependency between countries. Some countries are dependent on POCs in neighboring countries to connect to the worldwide web, outside of its own borders. For example, a Georgian accidentally severed a fiber while scavenging for metals, which in turn created a twelve-hour Internet outage for the neighboring country of Armenia. Though this incident was inadvertent, the same outcome could have been achieved by Georgia deliberately.

Points before and after the AS level in the physical communication chain, such as the fiber between Georgia and Armenia, can also be chokepoints, or arguably "points of control." Considering that situation, one should recognize that the “Point of Control” moniker used by Roberts and Larochelle refers only to number of POCs and not to all potential chokepoints in the Internet ecosystem. Furthermore, to reiterate what was mentioned when discussing the Roberts and Larochelle’s POCs and the CAIDA data on which their work is based, even the calculation of POCs itself is subject to some amount of error (2010).

Political Internet control likewise can be appraised in a number of ways. My operationalization (a blend of the scores from OpenNet Initiative and Reporters Without Borders) is also limited by what it does not incorporate.

Conclusion

The NPR classifications shed light on which countries may be more resilient to Internet disruptions by their governments. This is a measure of internal power of a country to control its own internet access. Future work assessing the resiliency to external force of neighboring countries on a given country is needed. Compiling measurements at all levels of Zittrain and Palfrey's (2008) control points would also be constructive. Automating measurements like these, where possible, would be useful in order to provide constant, up-to-date information. Resiliency data changes often due to the fast-changing nature of Internet connectivity, censorship technologies, censorship circumvention technologies and the dynamic nature of political situations. As measurements become more precise, more robust and more easily collected and compiled, NPR or other cumulative measurements can be a useful indication to international net neutrality and human rights organizations.

References

CAIDA. (2010, February 28). *AS Core Network*. Retrieved from CAIDA: http://www.caida.org/research/topology/as_core_network/

CAIDA. (2009, September 20). *AS Relationships Dataset*. Retrieved from CAIDA: http://www.caida.org/data/active/as-relationships/

Chuang, J. (2011 Spring). Lecture for "Computer-Based Communications Systems and Networks" course, School of Information, University of California, Berkeley.

Deibert, R., Palfrey, J. Rohozinski, R., Zittrain, J., Eds. (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press, 2008.

Dimitropoulos, D., Krioukov, D., Fomenkov, M., Huffaker, B., Hyun, Y., Claffy, K., et al. (2007). AS Relationships: Inference and Validation. *ACM SIGCOMM Computer Communication Review (CCR) , 37* (1), pp. 29-40.

OpenNet Initiative. (n.d.). *Global Internet Filtering Map*. Retrieved May 1, 2011, from OpenNet Initiative: http://map.opennet.net

Reporters Without Borders. (2011). *Internet Enemies.* Retrieved from Reporters Without Borders: http://march12.rsf.org/i/Internet_Enemies.pdf

Roberts & Larochelle. (n.d.). *CAIDA : research : topology : rank_as*. Retrieved April 28, 2011, from Cooperative Association for Internet Data Analysis (CAIDA): http://www.caida.org/research/topology/as_core_network/

Roberts, H., & Larochelle, D. (2010). *Mapping Local Internet Control, Unpublished raw data.* Retrieved April 28, 2011 from Berkman Center for Internet & Society at Harvard University: http://cyber.law.harvard.edu/netmaps/

Warf, B. (2010). Geographies of global Internet censorship. *GeoJournal* (76), 1-23.

Wikipedia (2011). *History of the Internet*. (2011, April 29). Retrieved from April 29, 2011, from Wikipedia: http://en.wikipedia.org/wiki/History_of_the_Internet

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. *MIT Press* , pp. 29-56.

Appendix 1 NPR (Network-Political Resiliency) Classification by Country

Source:	*OpenNet Initiative (2011 data)*		*Reporters Without Borders (2011)*	*Roberts & Larochelle (2010)*	*Calculated by authors*	
Country	**Political [Internet] Filtering Level**	**Total Internet Filtering Level**	**Enemies of the Internet**	**Points of Control (POC)**	**POC Redundancy Level**	**Network-Political Resiliency (NPR)**
United Kingdom	0	0	no data	78	High	**High**
Belgium	no data	no data	no data	13	Moderate	**Moderate**
Bulgaria	no data	no data	no data	32	Moderate	**Moderate**
Canada	0	0	no data	17	Moderate	**Moderate**
Czech Republic	no data	no data	no data	30	Moderate	**Moderate**
Denmark	0	0	no data	18	Moderate	**Moderate**
Germany	0	0	no data	24	Moderate	**Moderate**
Greece	no data	no data	no data	13	Moderate	**Moderate**
Hong Kong	no data	no data	no data	13	Moderate	**Moderate**
Hungary	0	0	no data	20	Moderate	**Moderate**
Italy	0	2	no data	26	Moderate	**Moderate**
Netherlands	no data	no data	no data	40	Moderate	**Moderate**
New Zealand	no data	no data	no data	13	Moderate	**Moderate**
Norway	0	0	no data	13	Moderate	**Moderate**
Poland	no data	no data	no data	19	Moderate	**Moderate**
Romania	0	0	no data	15	Moderate	**Moderate**
Slovakia	no data	no data	no data	13	Moderate	**Moderate**
Sweden	0	0	no data	44	Moderate	**Moderate**
Switzerland	no data	no data	no data	28	Moderate	**Moderate**
Ukraine	0	0	no data	47	Moderate	**Moderate**
Albania	no data	no data	no data	6	Very Low	**Low**
Algeria	0	0	no data	2	Very Low	**Low**
Angola	no data	no data	no data	5	Very Low	**Low**
Argentina	no data	no data	no data	8	Low	**Low**
Aruba	no data	no data	no data	1	Very Low	**Low**
Austria	no data	no data	no data	11	Low	**Low**
Azerbaijan	2	4	no data	1	Very Low	**Low**
Bahamas	no data	no data	no data	2	Very Low	**Low**
Bangladesh	0	0	no data	3	Very Low	**Low**
Barbados	no data	no data	no data	2	Very Low	**Low**
Belize	no data	no data	no data	1	Very Low	**Low**
Bermuda	no data	no data	no data	4	Very Low	**Low**
Bolivia	no data	no data	no data	3	Very Low	**Low**
Bosnia and Herzegovina	no data	no data	no data	5	Very Low	**Low**
Brazil	no data	no data	no data	9	Low	**Low**
Brunei Darussalam	no data	no data	no data	1	Very Low	**Low**
Burkina Faso	no data	no data	no data	2	Very Low	**Low**
Cambodia	no data	no data	no data	11	Low	**Low**

Source:	*OpenNet Initiative (2011 data)*		*Reporters Without Borders (2011)*	*Roberts & Larochelle (2010)*	*Calculated by authors*	
Country	**Political [Internet] Filtering Level**	**Total Internet Filtering Level**	**Internet Enemies**	**Points of Control (POC)**	**POC Redundancy Level**	**Network-Political Resiliency (NPR)**
Cameroon	no data	no data	no data	2	Very Low	**Low**
Cayman Islands	no data	no data	no data	2	Very Low	**Low**
Chile	no data	no data	no data	5	Very Low	**Low**
Colombia	0	0	no data	5	Very Low	**Low**
Costa Rica	no data	no data	no data	2	Very Low	**Low**
Cote d'Ivoire	no data	no data	no data	4	Very Low	**Low**
Croatia	0	0	no data	7	Low	**Low**
Cyprus	no data	no data	no data	8	Low	**Low**
Dominica	no data	no data	no data	1	Very Low	**Low**
Dominican Republic	no data	no data	no data	2	Very Low	**Low**
Ecuador	no data	no data	no data	8	Low	**Low**
El Salvador	no data	no data	no data	3	Very Low	**Low**
Estonia	no data	no data	no data	7	Low	**Low**
Faroe Islands	no data	no data	no data	2	Very Low	**Low**
Fiji	no data	no data	no data	2	Very Low	**Low**
Finland	0	0	no data	10	Low	**Low**
French Polynesia	no data	no data	no data	1	Very Low	**Low**
Gabon	no data	no data	no data	1	Very Low	**Low**
Georgia	2	4	no data	3	Very Low	**Low**
Ghana	no data	no data	no data	7	Low	**Low**
Gibraltar	no data	no data	no data	2	Very Low	**Low**
Guam	no data	no data	no data	2	Very Low	**Low**
Guatemala	no data	no data	no data	5	Very Low	**Low**
Haiti	no data	no data	no data	4	Very Low	**Low**
Honduras	no data	no data	no data	6	Very Low	**Low**
Iceland	no data	no data	no data	3	Very Low	**Low**
India	2	8	no data	4	Very Low	**Low**
Indonesia	2	7	no data	12	Low	**Low**
Iraq	0	0	no data	2	Very Low	**Low**
Ireland	no data	no data	no data	8	Low	**Low**
Israel	0	0	no data	3	Very Low	**Low**
Jamaica	no data	no data	no data	2	Very Low	**Low**
Japan	no data	no data	no data	9	Low	**Low**
Jordan	2	2	no data	3	Very Low	**Low**
Kazakhstan	2	4	no data	2	Very Low	**Low**
Kenya	no data	no data	no data	4	Very Low	**Low**
Kyrgyzstan	2	4	no data	3	Very Low	**Low**
Laos	no data	no data	no data	3	Very Low	**Low**
Latvia	0	0	no data	5	Very Low	**Low**

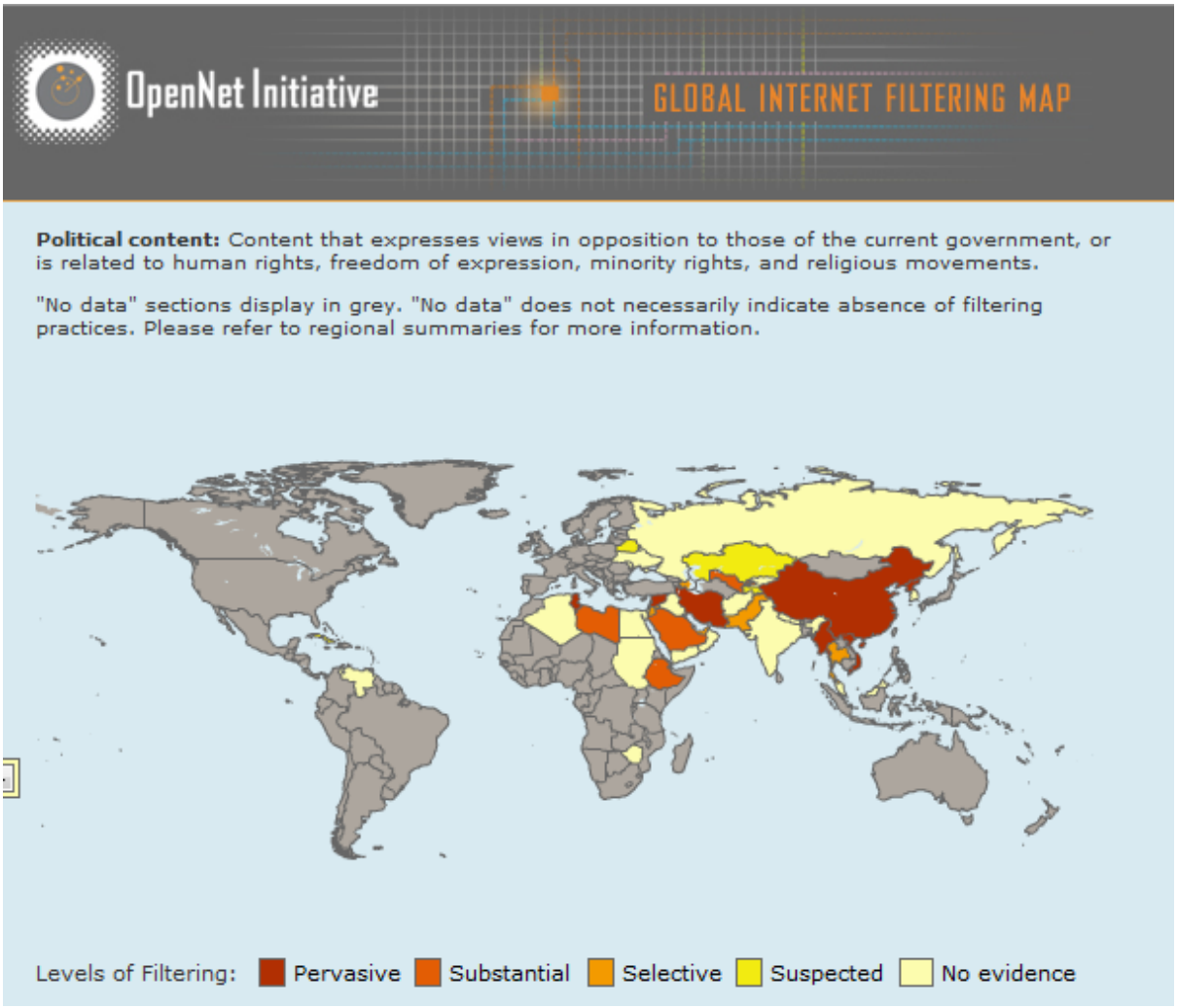
Source:	*OpenNet Initiative (2011 data)*		*Reporters Without Borders (2011)*	*Roberts & Larochelle (2010)*	*Calculated by authors*	
Country	**Political [Internet] Filtering Level**	**Total Internet Filtering Level**	**Internet Enemies**	**Points of Control (POC)**	**POC Redundancy Level**	**Network-Political Resiliency (NPR)**
Lebanon	0	0	no data	7	Low	**Low**
Liechtenstein	no data	no data	no data	4	Very Low	**Low**
Lithuania	no data	no data	no data	8	Low	**Low**
Luxembourg	no data	no data	no data	7	Low	**Low**
Macao	no data	no data	no data	1	Very Low	**Low**
Macedonia	no data	no data	no data	2	Very Low	**Low**
Maldives	no data	no data	no data	2	Very Low	**Low**
Malta	no data	no data	no data	2	Very Low	**Low**
Mauritius	2	2	no data	1	Very Low	**Low**
Mexico	0	2	no data	5	Very Low	**Low**
Moldova	no data	no data	no data	5	Very Low	**Low**
Monaco	no data	no data	no data	1	Very Low	**Low**
Mongolia	no data	no data	no data	2	Very Low	**Low**
Morocco	0	0	no data	2	Very Low	**Low**
Mozambique	no data	no data	no data	2	Very Low	**Low**
Namibia	no data	no data	no data	3	Very Low	**Low**
Nepal	0	0	no data	4	Very Low	**Low**
Netherlands Antilles	no data	no data	no data	4	Very Low	**Low**
New Caledonia	no data	no data	no data	1	Very Low	**Low**
Nicaragua	no data	no data	no data	5	Very Low	**Low**
Nigeria	0	0	no data	11	Low	**Low**
Oman	2	9	no data	1	Very Low	**Low**
Pakistan	2	9	no data	2	Very Low	**Low**
Panama	no data	no data	no data	3	Very Low	**Low**
Papua New Guinea	no data	no data	no data	1	Very Low	**Low**
Paraguay	no data	no data	no data	1	Very Low	**Low**
Peru	0	0	no data	3	Very Low	**Low**
Philippines	0	4	no data	5	Very Low	**Low**
Portugal	no data	no data	no data	10	Low	**Low**
Puerto Rico	no data	no data	no data	8	Low	**Low**
Rwanda	no data	no data	no data	2	Very Low	**Low**
Serbia and Montenegro	no data	no data	no data	3	Very Low	**Low**
Singapore	0	2	no data	12	Low	**Low**
Slovenia	no data	no data	no data	5	Very Low	**Low**
South Africa	no data	no data	no data	5	Very Low	**Low**
Spain	no data	no data	no data	11	Low	**Low**
Sudan	2	8	no data	2	Very Low	**Low**
Suriname	no data	no data	no data	1	Very Low	**Low**
Taiwan	no data	no data	no data	7	Low	**Low**
Tajikistan	2	2	no data	4	Very Low	**Low**

Source:	*OpenNet Initiative (2011 data)*		*Reporters Without Borders (2011)*	*Roberts & Larochelle (2010)*	*Calculated by authors*	
Country	**Political [Internet] Filtering Level**	**Total Internet Filtering Level**	**Internet Enemies**	**Points of Control (POC)**	**POC Redundancy Level**	**Network-Political Resiliency (NPR)**
Tanzania	no data	no data	no data	11	Low	**Low**
Trinidad and Tobago	no data	no data	no data	2	Very Low	**Low**
Uganda	0	0	no data	3	Very Low	**Low**
Uruguay	no data	no data	no data	3	Very Low	**Low**
Armenia	3	9	no data	3	Very Low	**Very Low**
Australia	0	0	Countries under surveillance	9	Low	**Very Low**
Belarus	2	8	Countries under surveillance	1	Very Low	**Very Low**
China	4	14	Internet Enemies	4	Very Low	**Very Low**
Cuba	2	4	Internet Enemies	1	Very Low	**Very Low**
Egypt	0	0	Countries under surveillance	6	Very Low	**Very Low**
Eritrea	no data	no data	Countries under surveillance	no data	Unavailable	**Very Low**
Ethiopia	3	8	no data	no data	Unavailable	**Very Low**
France	0	0	Countries under surveillance	11	Low	**Very Low**
Iran	no data	no data	Internet Enemies	2	Very Low	**Very Low**
Kuwait	2	12	no data	7	Low	**Very Low**
Libya	no data	no data	Countries under surveillance	1	Very Low	**Very Low**
Malaysia	0	0	Countries under surveillance	6	Very Low	**Very Low**
Myanmar	4	13	Internet Enemies	no data	Unavailable	**Very Low**
North Korea	no data	no data	Internet Enemies	< 4 *	Very Low	**Very Low**
Qatar	2	12	no data	2	Very Low	**Very Low**
Russia	no data	no data	Countries under surveillance	36	Moderate	**Very Low**
Saudi Arabia	2	12	Internet Enemies	8	Low	**Very Low**
South Korea	no data	no data	Internet Enemies	< 4 *	Very Low	**Very Low**
Sri Lanka	0	0	Countries under surveillance	5	Very Low	**Very Low**
Syria	no data	no data	Internet Enemies	2	Very Low	**Very Low**
Thailand	2	6	Countries under surveillance	14	Moderate	**Very Low**

Source:	*OpenNet Initiative (2011 data)*		*Reporters Without Borders (2011)*	*Roberts & Larochelle (2010)*	*Calculated by authors*	
Country	**Political [Internet] Filtering Level**	**Total Internet Filtering Level**	**Internet Enemies**	**Points of Control (POC)**	**POC Redundancy Level**	**Network-Political Resiliency (NPR)**
Tunisia	2	12	Countries under surveillance	no data	Unavailable	**Very Low**
Turkey	2	6	Countries under surveillance	2	Very Low	**Very Low**
Turkmenistan	4	10	no data	no data	Unavailable	**Very Low**
United Arab Emirates	3	13	Countries under surveillance	3	Very Low	**Very Low**
Uzbekistan	4	10	no data	9	Low	**Very Low**
Venezuela	0	0	Countries under surveillance	4	Very Low	**Very Low**
Vietnam	4	9	no data	4	Very Low	**Very Low**
Yemen	3	12	no data	1	Very Low	**Very Low**

* 3 POCs for "Korea, Republic of", not separated by North Korea and South Korea

Appendix 2 OpenNet Initiative's Global Internet Filtering Map – Political Filtering



Appendix 3 Reporters Without Borders Map of Cyber-Censorship