Research Report for MUNOH2014

Forum: Special Commission

Question of: The internet's role in providing democratic information and supporting democratic development

Student: Robin Groth, Gymnasium Meiendorf, Hamburg

Position: Vice President of the Special Commission

Description of the issue

In December 2012, the whole world began to look towards the Arabic World as thousands of enraged people took the streets to protest against their autocratic governments. They demanded a change in the social and political structures - a change towards democracy. They wanted to have a say in their country. This political discontent was partly sparked by whistle-blowing websites such as WikiLeaks, which had previously published documents revealing corruption and self-enrichment cases of the Tunisian government. Furthermore, the protests were largely organized via social media and would have been nearly impossible without them.This example demonstrates the democratic potential of the internet and it is now impossible to deny the network's strength and influence.

The web is so powerful in autocratic systems because it offers the opportunity to share and spread information on government wrong-doings, such as bribery and corruption, which cannot be done through state-controlled media. But we have to keep in mind that the web, as a free environment, creates new opportunities not only for the good but also for the bad. Of course, it can be used in democracies to ensure a high degree of transparency and make the people's participation in the democratic progress easier. However, it can also be abused by dictators to influence the public opinion by restricting access to oppositional web pages. After having experienced the strength of the web in the Arab Spring, autocrats now fear to be toppled themselves and try to tighten their grip on the internet. This becomes evident in the following case:

In spring this year, political opponents of Recep Tayyip Erdogan, the prime minister of Turkey, disclosed secretly recorded phone calls via the social media sites YouTube and Twitter. The records revealed cases of corruption prompting the opposition to organize protests and accuse Mr Erdogan of being a cormorant. Subsequently, Mr Erdogan censored the social media website Twitter and threatened to do the same with YouTube. During a public speech Mr Erdogan stated his aim to "eradicate Twitter and the like" and made clear that "the international community can say this, can say that" but he would not care. As the Declaration of Human Rights guarantees that "everyone has the right to freedom of opinion and expression" the intervention of Mr Erdogan should be seen with concern, as it poses a violation of the human rights.

Definition of Key Terms

When we talk about such a complex issue, it is important to clarify several technological terms:

Internet, Web

The internet provides the infrastructure necessary for the web. One could draw the analogy to our transport system: here the internet would be represented by streets and traffic lights and the web by vehicles such as cars and trucks. Please be aware that these two terms are not the referring to the same!

IP address

The Internet Protocol Address is a numerical label assigned to all devices that are participating in a computer network (computers, smartphones, printers etc.), so that those devices can be identified and information distributed among them.

URL

The Uniform Resource Locator (better known as web address) is a character string belonging to a web page, such as "http://munoh.de".

Techniques for internet censorship

Unlike in countries such as North Korea and Cuba, where the internet is completely state controlled, total censorship of information is nearly impossible to realize. The most commonly used techniques to filter information are:

- **IP Blocking:** access to a certain IP address is denied, thereby all websites on the same server are blocked. When the IP of a personal computer is blocked, all future connection attempts will fail.
- **DNS filtering and redirection:** domain names are not resolved and IP addresses returned incorrectly, the requested website cannot be viewed
- **URL filtering**: requested URLs are scanned for blocked keywords (in China these are inter alia: "police brutality", "Tiananmen Square protests of 1989", "freedom of speech" and "democracy")
- **Packet filtering:** monitoring method to see if suspicious keywords are going through the networks, connected web pages will then be blocked
- **Connection reset:** the connection from both sides is blocked by the firewall, usually for up to 30 minutes

Splinternet

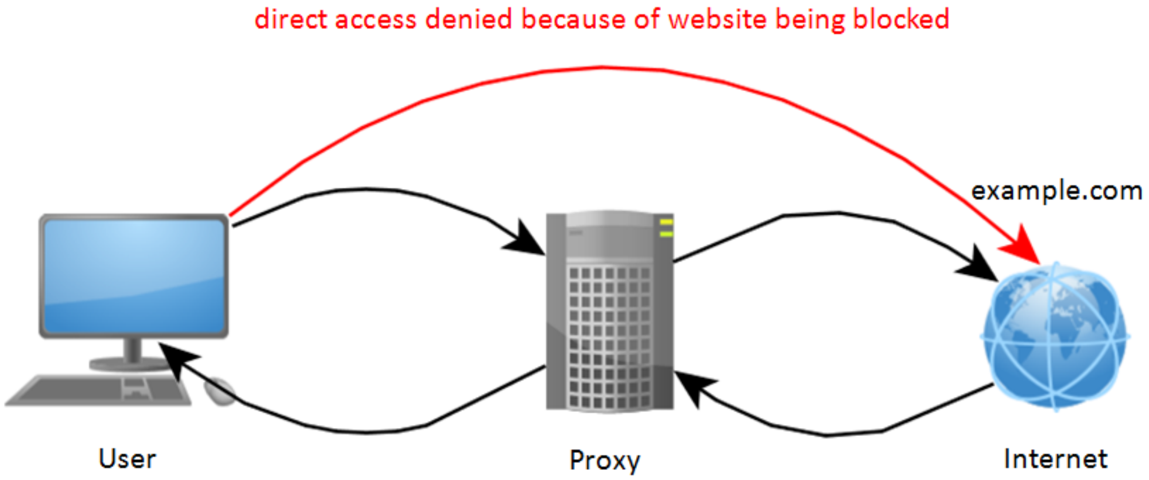
The term "splinternet" describes the network as being split and divided into several sub-networks which are separated by state-controlled firewalls. These firewalls prevent users from accessing information in the rest of the web. The "Golden Shield Project" (or commonly known as the "Great Firewall of China") in China for instance, was implemented because of political reasons. Chinese officials claim to protect and enhance China's stability in this way. Some other countries, among them the USA and Australia, plan to erect similar firewalls to block child pornography and weapon-making instructions.

Self-censorship

Companies like Google, YouTube or Twitter search their database on information that is not going to be tolerated by local authorities and censor that certain piece of information themselves.

Proxies

Internet users in countries like China try to bypass the local firewall in order to get access to the rest of web. The most commonly used method are proxies through which you navigate your internet traffic in order to view information which is blocked otherwise. The principle is schematically shown in the following picture[1]:



TOR

The Onion Router is a free software with the purpose of providing online anonymity and bypassing censorship. By channeling data through several "relays" it is nearly impossible to

[1] created with yEd

trace back the user who requested the blocked information. The network is of crucial importance for opposition movements in Iran and Egypt. Also journalists heavily rely on such software when reporting from undemocratic and suppressive countries.

Net Neutrality

The principle of net neutrality shall ensure non-discrimination on the internet. More precisely, this means that every data packet send through the network should be transmitted with the same speed regardless of its content and who sends and receives it. This principle is meant to guarantee everyone's right to express them freely on the internet.

Additional Terms

More important terms can be found under http://surveillance.rsf.org/en/glossary/#net

Background & General Information

Historical Development

In 1989 Tim Berners-Lee came up with an idea that would revolutionise the world. "Vague, but exciting" was his supervisor's remark to his proposal of a web in which information could be linked through hypertext. The web's initial purpose was to facilitate cooperation between several thousand scientists and researchers at CERN, the European Centre on Nuclear Research in Switzerland, by providing freely available information. Two years later on 6 August 1991, his idea became reality with the first web page being launched at info.cern.ch. Since then the web has undergone a rapid development. In its today's ubiquitous, diverse and functional form it has become a tool we use daily. However, the web diverged from its initial principle to provide free information. With the emergence of Facebook and alike, a process of commercialisation has begun, in which business models are arising that rely on locking information away from the rest of the world – instead of sharing it with everyone.

It may seem that for such a critical network it is inevitable to have commercialisation and government control. Several net activists, among them Tim Berners-Lee, have countered that perception. They want to preserve the internet as a democratic tool with open data available to everyone. To achieve this goal it is necessary to prevent political as well as commercial influence from entering the web and to protect our fundamental rights to privacy and freedom of opinion and association online. With commercial experimentation being continued and ever more governments being interested in censorship, their ideology is going to be tested.

Enemies of the internet – State Censorship

Some governments try to tighten their control on the internet which sparks unrest under net activists and journalists reporting from autocratic countries and therefore heavily rely on the network in order to spread information. *Reporters Without Borders*, an NGO, labelled twelve countries as “enemies of the internet” in a report published in 2010. According to the report, the situation of the Human Right to Freedom of Expression on the internet is worst in the following countries: Saudi Arabia, Burma, China, North Korea, Cuba, Egypt, Iran, Uzbekistan, Syria, Tunisia, Turkmenistan and Vietnam. The report distinguishes between countries that try to keep the population away from the internet by slowing down infrastructure development, like Burma, North Korea, Cuba and Turkmenistan, and those that are using heavy filtering systems to prevent unwanted information from accessing their internets. Filtering systems are for example used in Saudi Arabia and Uzbekistan, where the internet should better be called intranet or Splinternet as it is almost completely separated from the rest of the world. The NGO also sets Russia and Turkey, who have recently shown a concerning increase in online media control, under the “Surveillance List”.

More Enemies of the Internet

Obviously, several states (especially autocratic ones) try to influence information provided online and thereby pose a severe threat to the Human Right to Freedom of Expression. But we should not focus too much on states when it comes to internet censorship. Businesses make huge profits by selling surveillance software, which can be used by governments to collect data about their citizens as well as to filter the net for unpleasant information. Ironically, most of these firms are based in countries where the internet can be seen as largely unregulated and free, like in France or USA. To prevent authoritarian governments from using such software, democratic governments could restrict the sale of surveillance software. Reporters Without Borders urged the UN’s Human Rights Council to adopt a convention, requiring all Member States to regulate the export of surveillance technology.

One company, Blue Coat, engendered criticism with its activism in Myanmar where they are supposed to be responsible for internet censorship. The company is based in the US and sells filtering and censorship software to countries like Myanmar and Syria. Additionally, Blue Coat provides its customers with network analysis systems which can be used to monitor online traffic and individual online behaviour. However, Blue Coat mainly focuses on protecting companies against web and network-based threats as well as data loss, which is legitimate business.

Freedom Online Coalition

In 2011, 15 governments signed the founding declaration of the Freedom Online Coalition (FOC), declaring that the Human Rights are the same online as well as offline. The Member States commit themselves to promote internet freedom and to condemn measures violating Human Rights online, especially when it comes to free expression, association, assembly and privacy. Moreover, the Coalition supports individuals whose human rights online are in danger. Since its foundation the Coalition has grown to 23 members.

Relevant Treaties & UN Resolutions

Human Rights Council: The promotion, protection and enjoyment of human rights on the Internet (A/HRC/20/L.13)

Founding Declaration of the Freedom Online Coalition: http://www.humanrights.gov/2012/11/20/freedom-online-joint-action-for-free-expression-on-the-internet/

Useful links

- "Reporters Without Borders" – Enemies of the Internet (2010): http://en.rsf.org/IMG/pdf/Internet_enemies.pdf
  Recent online issue: http://surveillance.rsf.org/en/
- Gold Shield Project
  http://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html
  http://certmag.com/the-great-firewall-how-china-polices-internet-traffic/
- Report on Google.cn's Self Censorship
  http://www.internetfreedom.org/files/Research/report-on-google.cns-self-censorship.html
- Freedom House (a think tank dedicated to political freedom)
  http://www.freedomhouse.org/issues/internet-freedom

Research Guide

As the internet is such a powerful tool which can easily be abused, it is important for the international community to set up rules on how the network should be treated so that the Human Right to Freedom of Expression and Opinion is not violated. At MUNOH2014 it will be your task to negotiate with other delegates on how to best enforce this fundamental right. To help you with your research, you should find answers the following questions:

Questions for the delegate

- Is the internet censored in your country? If so, in which ways exactly?
- How is your government justifying censorship in the internet?
- Which political system is to be found in your country? Are free elections held?
- Can you find arguments supporting your country's position?
- How is your country dealing with other governments that are censoring the internet?
- What kind of steps could the UN initiate in order to prevent cyber censorship?
- How can the Right to Freedom of Expression be guaranteed on the internet?

Please send your position papers and resolutions to **specialcom@munoh.de** before the deadline on August 29. If you face any difficulties, please do not hesitate to contact us.