African Union
Peace & Security Council

By Harald Rutsch

Research Report

The Question of:

Limiting Internet access for security reasons

Introduction

In recent years it has become more commonplace for African nations to slow, restrict, or block access to the Internet. Most incidences of such tampering with the Internet have been recorded in cases of terroristic attacks, mass protests, or civil unrest. In most of the incidences, all involved governments claimed that any tampering with the internet was due to national security.

After the 2011 "Arab Spring" movement, which was largely organized over the internet (and in particular over social media), many governments have become wary of the Internet. This has led to aggressive use of censorship, particularly of anti-government activity. The 2011 "Arab Spring" movement resulted in the "Arab Winter" and many of the prevalent conflicts in Africa.

Many freedom and rights activists claim that the government's censorships infringe on the rights of the freedom of press and freedom of information. Furthermore, they also claim that governments have started abusing their power for personal and political reasons.

Especially in recent times, it has become commonplace in some nations to tamper with the internet in the lead-up to elections. Social media, in particular, are a popular target for restrictions. Governments claim that these restrictions are necessary to maintain the integrity of their elections but have failed to produce any evidence linking justifying these bans adequately.

The Committee

Definition and History

The African Union's Peace and Security Council (AU PSC) is an advanced ad hoc committee. As stated on their website it has the following mission and obligations: " The Peace and Security Council (PSC) is the standing decision-making organ of the AU for the prevention, management, and resolution of conflicts. It is collective security and early warning arrangement intended to facilitate timely and efficient responses to conflict and crisis situations in Africa. It is also the key pillar of the African Peace and Security Architecture (APSA), which is the framework for promoting peace, security, and stability in Africa." The AFPSC is comparable to the UN Security Council with the exception of the P5 (*Note: The AU is NOT part of the UN*).

As stated on the AU website: "The Protocol Relating to the Establishment of the Peace and Security Council was adopted on 9 July 2002 in Durban, South Africa, and entered into force in December 2003. The PSC became fully operational in early 2004. The PSC Protocol, together with the PSC Rules of Procedure, the AU Constitutive Act and the conclusions of various PSC retreats, provide operational guidance to PSC activities." The AU replaced the Organization of African Unity (OAU) which did little to protect citizens' rights and was dominated by dictators. The AU was founded under the leadership of Libyan head of state Muammar al-Gaddafi which together with other OAU members issued the Sirte declaration. The declaration was followed by a summit in Lomé in 2000 where the constitution of the AU was adopted. In 2001 at Lusaka the plan for the implementation for the AU was established. The AU began operations in 2004.

Procedure

The AU PSC is an ad hoc committee. This means that there will be no lobbying, therefore we ask you to prepare amendments for debates. The resolution will be created during the debate with amendments meaning that we start with a blank page. There are no “P5” countries in the committee and no vetos. All votes require a two-thirds majority to pass. The AU PSC can take actions which are binding for all members including the deployment of troops. All motions including follow-ups are at the discretion of the chairperson. For more detail relating to procedure during debate please refer to the THIMUN rules of procedure.

Key Terms

ISP

Internet Service providers (ISPs) are companies which provide internet service in any shape or form. ISPs often own large amounts of infrastructure; this lets them provide services to many users. There are several different types of ISPs but they can be classified into different categories: Mobile-Network ISPs, Traditional-ISPs, and Backbone ISPs. A Mobile-Network ISP is often tied to a telephone service provider and provides Internet for mobile devices such as phones. Traditional-ISPs are companies that provide Internet to homes and businesses; they often own vast networks of fiber optics. (Traditional ISPs sometimes use telephone and TV cables for the last hundred meters especially in older cities and towns.) Backbone ISPs provide network infrastructure services to large corporations, other ISPs, and governments. Backbone ISPs own intercity cables, undersea cables, satellites, and large internet exchanges. Note: These are not strict categories, and many ISPs have ventures in multiple categories. For example: the Dutch ISP KPN provides service to homes and businesses. It also supplies mobile Internet and provides the Dutch government with the Internet.

Social Media

Social Media are applications and websites designed to enable users to create, share, and comment on information, ideas, and other interests. Due to the large diversity of social media, no precise definition can be made.

Social Media use during the "Arab Spring"

During the "Arba Spring" movement many of the large-scale protests were organized with the help of social media, specifically Facebook. Many experts claim that social media played a crucial role in the uprising. Social media also enabled fast communication during the protest, leading to fast responses from a growing crowd. The use of social media also enabled unprecedentedly fast communication between different protest groups.

VPN

Virtual Private Networks (VPNs) are applications that create a secure connection to a private network over a public network. Set applications achieve this by establishing an encrypted point-to-point connection with tunneling protocols to a remote network. VPN technology was developed for corporate use and is used by almost all large corporations to communicate securely between regional and HQ offices, and for employees that are roaming (for example, working at home or on a laptop.) In recent years VPNs have become popular amongst people who are trying to circumvent internet restrictions set out by their governments. Many people use commercial VPN services to connect to foreign countries and use the internet provided through the VPN.

General Overview

The issue presented here has multiple aspects which might be irrelevant for some member-states, but in order to provide a general easy-to-navigate overview, it will be presented in multiple parts divided by clear titles. However, it is still highly encouraged that every member state also studies their own situation in order to be informed of their stance in this matter.

The positive impact of restricting the Internet

Every government on the planet has the obligation to maintain its rules and restrictions, therefore it is crucial that illegal material such as, but not limited to, illegal substances, child pornography, and illegal weapons is monitored and restricted in accordance to the laws of the nation.

It is important to note that this must be accomplished while maintaining the rights of the people.

In some cases, tampering with the Internet during or after a crisis situation might be a necessity to resolve the crisis or consequences of the crisis. But the ability to use these actions must be regulated and must have some form of accountability to ensure no rights are being violated and no misuse occurs.

Political usage of the Internet

There are multiple political usages of the Internet but only the most popular will be presented.

Tampering with the domestic Internet for political power

Most governments want to stay in power and some governments have always used methods which violate human rights. The Internet is no exception; controlling it is a method that governments have used as a means of violating human rights. Even before 2011 cases of tampering with the Internet existed, the very first being in February 1996 in Zambia. The government of Zambia successfully forced their biggest ISP Zamnet to remove a band edition of "The Post" with was deemed illegal under the "Preservation of the Public Security act" because the report allegedly contained information based on leaked documents which revealed government plans on the adoption of a new constitution. The government achieved this by threatening legal action against the ISP. In the end effect, the government's actions were rendered ineffective because a US reader posted the edition on his own site, over which the Zambian government has no jurisdiction. Almost all cases of government-lead censorship proceeded in a similar fashion to this case. The general consensus around the Internet was~~ a~~ positive ~~one~~; almost no government saw the unregulated Internet as a threat to them. But after the events of the 2011 Arab Springs, some states changed their views. The by far biggest change was selected states' views on social media.

Social media was one of the most important drivers of the "Arab Spring" revolutions; as a result, many governments tried implementing measures to limit negative exposure, especially on social media sites. Most affected were governments with leaders that have been in power for a longer period of time. One of the most common measures of limiting negative exposure is blocking social media platforms as soon as any negative conflict arises. One example is the 2016 Presidential race in Uganda, in which the President Yoweri Museveni, who had already been in power since 1986 (30 years), won reelection. Prior to and during the vote Mr. Museveni's government shut down almost all forms of social media. Mr. Museveni defended the practice by stating the following: "security measure to avert lies ... intended to incite violence and illegal declaration of election results." Many Internet rights activists and foreign experts claim that the action was a violation of-freedom of speech. The most extreme case of restricting social media occurred in Chad where the government blocked all access to social media for 16 months. (Long restrictions or shutdowns are usually not used because of their large economic impact.)

Slowing down services on the Internet is the most common tactic used by governments. This method aims to deter usage by frustrating the user. The problem with identifying this method is that bad infrastructure can be easily be blamed for the slowdowns. It is unclear if this method has deterred any anti-government action.

Many Internet rights activists and experts claim that the governments which employ methods of tampering with the Internet are actively infringing in the rights of the freedom of speech and expression, and have abused ~~the~~ executive power for their own political and personal gain. (It is worth noting that not all African countries have had a record of tampering with the Internet.)

Tampering with the Internet by foreign or unknown powers

It is no secret that states have always tried to influence other states to gain advantages, or to inflict damage . In an age where almost everything relies on computers, this has become easier than ever. The most well-known and well-documented case is Russia's interference in the 2016 USA election. The government of the USA has published reports showing the extent of Russia's interference. The reports outline how social media platforms were used to identify people which had been deemed undecided or politically vulnerable and then used to gain information to deliver targeted ads to influence their opinion.

While manipulation of the masses is by far the most open way to tamper with democracy, many other ways exist. The most common way state and non-state actors try to influence nations are by cyber attacks most often directed at the governments and their services. The most well-known example in recent history is the attack of ransomware called "WannaCry". WannaCry was ransomware that was made by two North Korean individuals. The attack exploited a weakness in older (not updated) versions of Windows, and encrypted all files demanding a ransom for decrypting them. Even if the ransom was paid the software still did not decrypt the information. This ransomware impacted many government systems around the world (most notably healthcare). These types of attacks are the most common and can harm every entity connected to the Internet. Governments and companies around the world are actively protecting themselves. Many African nations use this activity as an argument to restrict the Internet, particularly around elections.

Major Parties Involved

Governments

Governments are the primary party controlling the outcome of this issue . They decide what rights the people have and have instituted bans, limitations, and control over the internet. Governments also have an obligation to protect their people from foreign attacks. Some governments have a history of abuse of power and tampering with the Internet.

ISPs

Internet Service Providers are the main tools for governments to control the internet. Every action regarding the internet has to be made through an ISP. Many ISPs have shown resistance to illicit government requests over the years but many governments have found ways to force ISPs to comply with their wishes. In some countries, there is only one government-owned ISP witch can easily be influenced by the government.

Non-state Actors (Hackers)

The Internet has made it possible for non-state actors to gain power. Non-state actors have the ability to harm Individuals, companies, and governments by launching cyber attacks. It is very hard for governments to track such parties. Non-state actors can have a multitude of reasons for their attack. Non-state actors attacks usually have a small to medium impact.

Foreign Governments

Foreign Governments usually target government functions and authorities. Their aim is to disrupt the function of the government. The motivation of each attack varies. Foreign governments may also try to misinform citizens to influence national or local politics. Foreign governments have a large number of resources, therefore their attacks usually have a medium to large impact.

Timeline of Events

February 1996, Zambia	The first recorded instance of governments restricting the Internet.
2011, Africa and Middle East	The Arab Spring movement changed the view of governments.
2016, USA	Russia tamped in the USA presidential election
2018-2019, Chad:	Chad blocked social media platforms for over 16 months (a record amount of time).

Previous attempts to solve the issue

There have been no previous attempts to resolve this issue.

The Future

Note: It is obviously impossible to predict the future, this is just my educated guess.

It is very likely that governments will continue to restrict the Internet. It is very unlikely that any governments will roll back their restrictions. Internet blackouts will become more common especially in times of protest. Governments which have a record of misusing their power for purposes not related to security will continue to misuse their power and will probably extend their power. Social networks will be under continued pressure to abide by governments' wishes regardless of the ethicality or legality of their request. In times of public outcry damaging a government's image, speech online will be restricted and social media suspended. Online media will face the same censorship as traditional media thus entailing a rise in the suppression of press freedom. With the amount of big data increasing cyber-attacks similar to the USA 2016 election tampering by Russia will become a larger threat. It is very likely that certain governments will start tracking individuals that speak out on the Internet.

Questions a Resolution Must Answer (Q.A.R.M.A.)

Here too it is important to make clear to the delegates that they should **not** limit themselves to only the questions standing here.

Since the threat of criminal activity is always growing is there a way to restrict the Internet for security reasons while maintaining the rights of the people and limiting improper government use.

- Can the AU PSC make any declaration about the status (condemn) of countries that violated the rights of the people?

- Can the AU PSC Member States comment on the threats of non-state actors trying to influence/harm people, governments, and governments by using the internet?

- How should governments that go against the council's demands and regulations be punished?

- How should governments punish people that have committed crimes related to the disruption and modification of governments services, companies, and people over the Internet?

- What does the council think about governments suppressing the freedom of speech on the Internet and blocking social media platforms during periods of negative speech regarding the government?

- Does the council have any thoughts on requiring governments to establish~~ing~~ oversight regarding the use of measures that modify the internet for security reasons?

- How should the AU PSC respond to large-scale cyber-attacks on one of its members?

- Should the AU PSC establish an intergovernmental panel to monitor governments use of methods that restrict the internet due to security reasons?

- How large is the threat level reading cyber terrorism and which countermeasures are appropriate?

Further Reading

https://pdfs.semanticscholar.org/1b36/4798ab570b61bbd858b1b5eb4e45911f236.pdf [I]
https://mashable.com/2014/12/17/internet-freedom-countries/#I__rGrhXWmqw[II]
https://freedomhouse.org/report-types/freedom-net[III]

Bibliography

https://en.wikipedia.org/wiki/Category:Internet_censorship_in_Africa
https://mg.co.za/article/2018-08-06-internet-censorship-in-africa-threatens-democracy-economy
https://www.bbc.com/news/world-africa-36024501
https://thebestvpn.com/are-vpns-legal-banned-countries/
https://money.cnn.com/2016/09/16/technology/internet-censorship-blackouts-gabon/
https://freedomhouse.org/report-types/freedom-net