IS INTERNET FRAGMENTATION ALREADY PART OF OUR REALITY?

Valeria Peddis

Analytica
FOR INTELLIGENCE AND SECURITY STUDIES

ANALYTICA FOR INTELLIGENCE AND SECURITY STUDIES

- CYBER SECURITY

IS INTERNET FRAGMENTATION ALREADY PART OF OUR REALITY?

Valeria Peddis

TURIN, MARCH 2023

www.analyticaforintelligenceandsecuritystudies.it

Analytica
FOR INTELLIGENCE AND SECURITY STUDIES

Introduction

The Internet is the perfect example of an interoperable world where networks need to cooperate with other networks to fulfil their aim: limitless communication. When it was born its freedom from governments' control was one of the main traits of this crucial web infrastructure. This trait made it hard for the law to regulate it.

Internet users often adopt voluntary standards proposed by the Internet Engineering Task Force (IETF), an international association of researchers and engineers created in 1986 in the United States of America, where the Internet is said to have been born. Today, the association comprises employees from all over the world, despite the huge disparity between the number of American employees and those of other nationalities.[1]

In the latest years we are experiencing what so called "Balkanization of the Internet". This is another way of addressing Internet fragmentation, a phenomenon that consists in creating various Internets. These different Internet versions are controlled by the governments within the borders of their jurisdiction. Having control means that the governors can select which information can be displayed to its users. This fragmentation is a two-fold situation, which can be seen as a risk for democratic countries while it can be a possible opportunity for authoritarianism and censorship to control their citizens. Even if this phenomenon is becoming a solid reality, some scholars believe that the Internet Protocol (IP) for communication will keep the Internet altogether. [2]

There are many ways of blocking Internet access among regional borders, both physical and digital. Four methods tend to be more used than others, they include: (1) technical blocking, (2) search result removals, (3) take-downs, and (4) induced self-censorship. Note that in the latter two cases, the blocked access is not considered to be permanent since the information remains available but is not accessible. During a take-down, citizens are not allowed to surf certain websites nor reach certain information if blocked by their country. In the case of induced self-censorship citizens are aware that if found surfing certain websites by the government, they could be exposed to significant risks. The implementation of these measures is generally not continuous. To block someone's access, a country can filter and redirects the DNS (Domain Name System, a technology that translates websites to IP addresses), in this case the user can redirected to different websites or can access just a part of the content they were looking for. Another technique is to block certain IPs or some URLs (Uniform Resource Locator), in those cases users, when trying to access it, can even receive a failure to connect message. Another way is to hide results if they contain specific words. Those listed techniques require a collaboration between countries and local Internet providers since these latter, according to government indications, must configure their services (e.g., setting routers) to reject access in certain cases and monitor users' Internet access.
Indeed, some countries may use a small level of censorship while others may use more pervasive censorship controls against their citizens (e.g., pervasive level of censorship occurs in countries like China, Syria, Iran, Vietnam, Myanmar, Turkmenistan, and Uzbekistan while in Saudi Arabia, Yemen, UAE, and Ethiopia there is a strong censorship even if it is slightly less pervasive than the one in above mentioned countries. Most of the other Asian countries, including Russia, apply a selective censorship policy).[1]

[1] Hill, J. F. (2012) Internet Fragmentation. Highlighting the Major Techincal, Governance and Diplomatic Challenges for U.S. Policy Makers. *Harvard University*
[2] Ryan, G. (2020). Shatter the web: Internet fragmentation in Iran. *Middle East Institute*
https://www.mei.edu/publications/shatter-web-internet-fragmentation-iran

Internet fragmentation, at first, seems a solution for cyber-attacks: a closed Internet is less vulnerable than an open one. But instead of building multiple closed Internet it is better to promote preventative plans in order to avoid attacks, or at least recover from them. Having every country manage IPs and DNSs can lead to blocked connections due to the impossibility of different systems to speak to one another.

Internet competition

The Internet, by definition, is a tool that can be used to have access to content from all over the world. This feature can be both positive or negative, depending on if we are watching it from a democratic country or from an authoritarian one. In fact, some authoritarian governments started to restrict and control Internet within their borders. This is the case of China and Russia.
China started to put the Internet under state control in 1996 with State Council Order n. 195. This norm requires devices to access the world wide web through a state-run "exit information channel" making it possible for the state to filter its content. For example, Chinese people might not be familiar with YouTube, but would rather mention "Bilibili", an app deliberately created to be used in China, where there is no international or Western influence in the content. Also WhatsApp has its Chinese version: WeChat. Not only apps, but newspapers like Times or the Journal have had the same treatment.
The Chinese censorship program, called the "Great Firewall", was first implemented in 2000 when the government started to acquire personal Internet records while restricting users' access to Internet[3]. There are various tools, like VPNs (Virtual Private Network), which make it simple to avoid the restrictions of the Great Firewall. Even if using a VPN is not illegal in China, many of them have been banned. Foreigners have never had problems using a VPN, however, in order to use a VPN, Chinese citizens need to provide a precise business reason, and obtain a permit to use it. China building its Internet can be viewed as an international issue not only because of the interconnections of the Internet itself but also because China has invested in African countries, such as South Africa, Angola, and Niger among others[4]. Those countries are likely to follow the Chinese lead to protect their investments. In addition to this, China is also planning to own a blockchain that will allow them to control every communication, especially online transactions, while creating a new digital currency similar to a digital yuan[5].
Similar to China, Russia also tends to implement censorship policies through the Internet, having started in 2012 when Roskomnadzor, the federal telecommunications regulator at that time, created a blacklist of prohibited sites. This register still exists today, requiring Internet service providers to block the listed sites to avoid being charged with hefty fines[6] One of Russia's strategies to block access to the Internet is self-censorship. For example, the Bloggers Law obliges bloggers having more than 3000 followers to register with the mass media regulator and take responsibility for the posted content and its reliability[7].

Looking instead at Iran, the government has deactivated Internet's access to its citizens in multiple instances to promote national interests, with the most recent example being the Amini protests during

[3] Wang, Y. (2020) In China, the 'Great Firewall' is changing a generation. *Human Rights Watch.* https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation
[4] Rolland, N. (2022) Political front lines: China's Pursuit of Influence in Africa https://www.nbr.org/publication/political-front-lines-chinas-pursuit-of-influence-in-africa-introduction/
[5] Kenyon, F. (2021) China's 'splinternet' will create a state-controlled alternative cyberspace. https://www.theguardian.com/global-development/2021/jun/03/chinas-splinternet-blockchain-state-control-of-cyberspace
[6] Lupion, M. (2021). *The Sino-Russian Digital Cooperations and its implications for Central Asia*. Kassenova & Duprey
[7] Russia enacts 'draconian' law for bloggers and online media. (2014). *BBC News.* https://www.bbc.com/news/technology-28583669

which the Internet became unavailable for six days. This procedure had already been used during the suppress the protests of 2020 and 2019. The country is well known for trying to build its own Internet since 2013, when the "NIN" (National Information Network) was created, although the first censorship attempts can be dated back to Mahmoud Ahmadinejad's governement[1]. The implementation of the NIN allows access only to a restricted Internet, while the "international Internet" cannot be reached by Iranians.

Conclusion

Even if there are ways to go beyond the Great Firewall, average users do not have the technical skills required to achieve this. Indeed, it is estimated that out of 500,000,000 users fewer than 1% of them can use those tools.[1]

Without access to foreign sources of news, it is easier for governments to manipulate and twist local news.
One of the risks of Internet fragmentation can be a future pricing schedule charged by Internet operators for services applied to the originating party (e.g., Google, Yahoo etc…) [8]
More democratic countries are now more reliant on technological components produced in China. Nowadays, China produces most of the micro-components of electronic devices, making it impossible to produce a phone without them. Their run for the fastest growth can limit democratic countries to a position of dependence on their services and devices.

International Internet associations can monitor the situation but sanctioning those countries can be counterproductive, e.g., Iran: the number of sanctions given by the USA led to a faster implementation of the NIN, after the sanctions the project was sold by the government as anti-imperialist struggle not as a tool of oppression[2].
To properly function, the Internet needs to connect with other systems. One could argue that recent developments have made it impossible to keep the Internet neutral or uncontrolled by governmental institutions.

There are various measures that can help counter misinformation, and controlled content propagated by state media, such as keeping student exchange programs open and allowing workers to go abroad to work. Volunteering work abroad is another social solution, those opportunities are often managed by NGOs or private stakeholders without any political affiliation. Even though governments play a pivotal role in these situations private organizations and non-profit initiatives can be change-makers too. Cultural exchanges, globalization and the need of worldwide customers or audience can delay Internet fragmentations from worsening.

International laws, if implemented, could be helpful to control Internet access and its usage, especially now that the splinternet is closer but not yet our reality. Dialog among both countries and non-state representatives (e.g., Internet providers) and diplomacy should try to prevent that from happening mainly because the Internet is becoming more and more a weapon of modern wars e.g., Russia's misinformation about the war in Ukraine or Ukraine demanding ICANN (Internet Corporation for Assigned Names and Numbers) to block .ru sites. Having Internet access is now predominantly considered a fundamental right as it provides essential services, such as buying goods, working, reading the news, and more. Thus, blocking Internet access can dramatically impact on somebody's life.

[8] Economides, N., Tag, J. (2011). *Network Neutrality on the Internet: A two sided market analysis.* NET Institute Working Paper. 07-45. NYU Law and Economics Research Paper.