H.E.I.P
AEROSPACE
CYBERSECURITY
DEF'INSEEC

Def'INSEEC
Aerospace & Cybersecurity Division

A New Internet ?

The Chinese and Huawei proposition for a new IP Protocol

Reading time: 7 min

The Future is on its way: 5G was activated in France by SFR on November 20th and Bouygues Telecom on December 1st. Yes, it has been launched and we will all soon be able to fully use 5G on all of our electronic devices by 2030 according to Numérama. But there are currently many debates about 5G, for example, could it be more dangerous than 3G and 4G for our health?

The answer is mainly no. The goal of 5G is to allow us to have a faster and more stable connection. The main source of concern is its radio beam. As the frequency is higher it does not travel as far as the 4G beam. Therefore, 5G requires more antennas and these antennas have to be closer to the ground. It is worth noting that this higher frequency beam, because of its increased efficiency, is potentially less dangerous for human bodies.

We are all concerned about wether the beam could impact our brain and provoke cancer. But no objective scientific studies have demonstrated such an effect. On the contrary, the International Agency for the Research on Cancer (IARC) of the World Health Organization (WHO) has qualified 3G and 4G as potentially carcinogenic.

Another issue is currently taking place : Guillaume Poupard, General Director of the French National Agency for the Security of Information Systems (NASIS, ANSSI) in an interview for Les Échos justified the decision to halt the Chinese Corporation Huawei by national sovereignty issues. Other references such as Numérama claim that Huawei could be used as a "Trojan Horse for Beijing to drive sabotage and spying operations" (Le Parisien) but nothing has been proven yet.

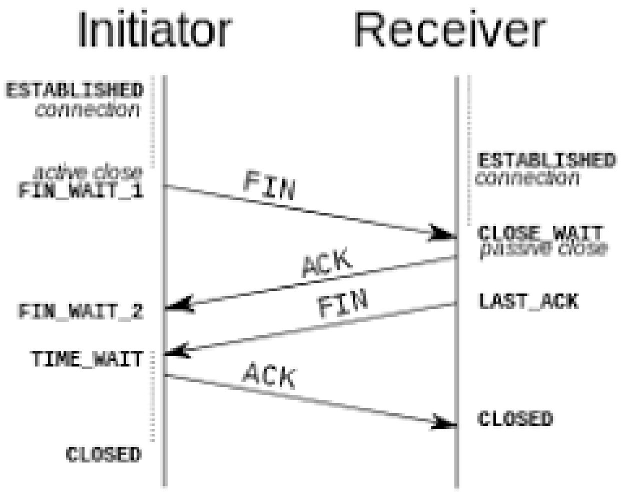
Another issue about Huawei is the future Chinese Internet Protocol. The Financial Times revealed in March 2020 in an article called "Inside China's controversial mission to reinvent the Internet" that Huawei presented before the United Nation and delegates from more than forty countries in September 2019 a new Internet Protocol called the New IP protocol.

What is this protocol? Who could be interested by this new protocol? What are its potential dangers? We will try to answer these questions one by one in order to explain everything we need to know about this proposition.

WHAT IS THIS PROTOCOL?

To understand what this New IP Protocol will bring, we first need to understand what an IT Protocol is. A protocol is commonly known as a set of rules, for example in a corporation, to interact with the hierarchy or to send a particular document. In the same idea, an IT Protocol is a set of rules allowing the swap of data between IT systems. The two main protocols organizing the Internet are:

- The **TCP Protocol**: TPC for Transmission Control Protocol. It asserts of the liability of the connexion for the transmission of data. A TCP session allows messages to be forwarded by a three-step procedure: establishment of the connexion, data transfer, closure of the connexion.



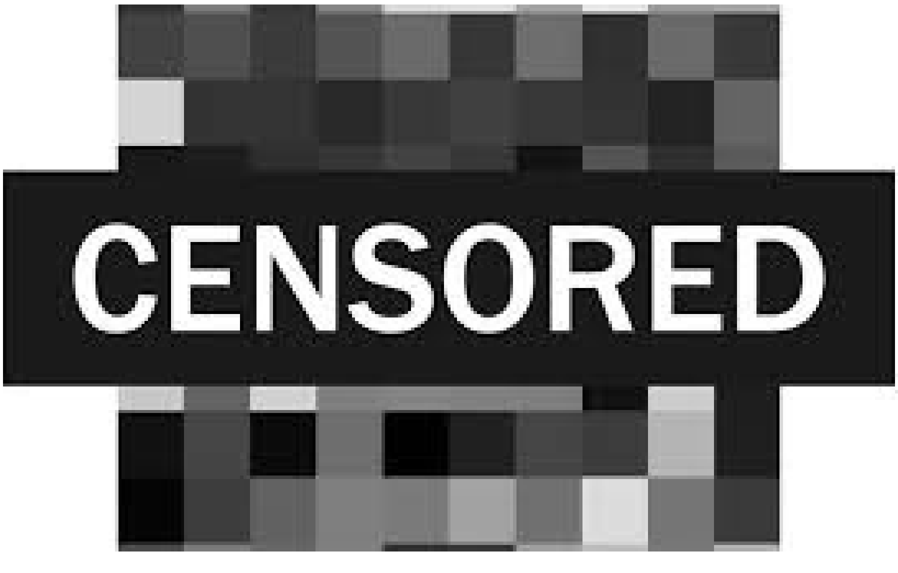
- The **IP Protocol**: the Internet Protocol completes the previous one by a logic of addressing. As machines communicate through networks, they have to find a path to exchange data. Therefore, the IP gives to every machines an IP address, allowing a unique identification of the machine and its localization.

The issue of the New Chinese IP Protocol is that it would replace the existing IP Protocols. The idea of Huawei is to gain a competitive advantage in the changing digital landscape with the future arrivals of holograms and self-driving cars. The New IP would ease the addressing and make it more effective.

WHO COULD BE INTERESTED BY THIS NEW PROTOCOL?

Saudi Arabia, Iran and Russia have already expressed their support of this evolution. Events in Iran and Saudi Arabia have already taken place providing a glimpse of what the new Internet would look like: A black out of Internet connectivity was prolonged during civil unrest allowing only access to essential services like baking and healthcare.

Russia adopted on November 2019 a "sovereign Internet" law allowing the government to monitor web traffic closely. Specifically, this law is another step toward the isolation of the Russian Internet network which already forbids the access to LinkedIn, Telegram or even Dailymotion in Russia. Such censorship is also used in Iran and Saudi Arabia and other countries of the region like the United Arab Emirates.



WHAT ARE THE POTENTIAL RISKS OF THIS NEW IP?

What alarmed the Financial Times is the introduction of a "kill switch" or "shut off". A kind of emergency stop button that would allow the principal actor, therefore the state, to block access of an IP address to the network. This address would then not be able to send or receive data anymore. But Huawei affirms that this "kill switch" has been created to stop any cyber-attacks.

Governments today agree on the fact that a new legal framework needs to be put in place to better manage Internet Governance. This new legal framework would give more regulatory control to the political and economic spheres and potentially provide a solution to the current fiscal loopholes used by the GAFAM. Laura Penardis (2014, The Global War for Internet) has described in detail the above problems and potential solutions.

Nowadays, we have two models of Internet:

- a market-led capitalist version based on surveillance and self-regulation,
- an authoritarian version based on surveillance and state-regulation.

By this proposition, China through Huawei wants to export its model of Internet which is a closed network blocking the Western Internet. But the real danger of this model is that it is designed for totalitarian impulses (Shoshana Zuboff, 2018, The Age of Surveillance Capitalism) allowing governments to close the gates for users according to, for example, their political opinions. It would also mean that everyone would need permission from their Internet provider to do anything via the Internet, wether downloading an app or accessing a site, and administrations could have the power to deny access on a whim.

Such a protocol would also induce a patchwork of World Wide Webs, each based on its own rules for their own cyber sovereignty.

The New IP Protocol could then be helpful for the future technological evolutions. But, there will be a problem for both democratic and authoritarian states. Allowing administrations to access your data and able to shut down access to the Internet is a dangerous deviation that should be strictly supervised by independent supra-national entities. To grant these entities such power could restrain governments from any arbitrary decision potentially dangerous for the freedom of speech.

The new IP protocol will be tested in 2021.What is now sure is that Western countries will need to keep up with these evolutions in order to stay economically and technologically competitive. The main question, according to the Financial Times here, is the following: will Europe and North America pull together to construct the legal and technical framework for a democratic alternative ?

Written by Guillemette Jahn,
Cybersecurity Manager of the Aerospace & Cybersecurity division

Edited by:

Anaëlle Le Lostec
Constance Alloy
Michael Ellison

Sitography:

https://www.leparisien.fr/high-tech/5g-cinq-minutes-pour-comprendre-la-mise-a-l-ecart-de-huawei-en-france-08-07-2020-8349573.php
https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html
https://www.lemonde.fr/international/article/2019/11/01/une-loi-sur-le-controle-d-internet-entre-en-vigueur-en-russie_6017729_3210.html
https://information.tv5monde.com/info/russie-que-va-donc-changer-la-loi-pour-un-internet-sur-et-durable-instauree-par-poutine-298499
https://www.phonandroid.com/huawei-et-la-chine-proposent-new-ip-une-mise-a-jour-dinternet-pour-les-regimes-autoritaires.html#:~:text=La%20Chine%20pr%C3%A9sente%20avec%20Huawei,la%20censure%20des%20r%C3%A9gimes%20autoritaires.
https://www.huawei.com/en/industry-insights/innovation/new-ip
https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

Follow Def'INSEEC on :

Def'INSEEC
Aerospace & Cybersecurity Division