INSTITUTE FOR POLITICS AND SOCIETY

elf

Building 5G Networks in Europe

ANALYSIS / OCTOBER 2019

ADÉLA KLEČKOVÁ
ROMAN MÁCA

WWW.LIBERALFORUM.EU

Published by the European Liberal Forum asbl with the support of the Institute for Politics and Society. Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the authors alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum asbl.

WWW.POLITIKASPOLECNOST.CZ

OFFICE@POLITICSANDSOCIETY.CZ

Content

Building 5G Networks in Europe

Analysis – Adéla Klečková, Roman Máca; October 2019

Preface

We rarely ever pass a day without hearing about the abbreviation "5G." It is supposed to be a revolution, enabling us to have all the amazing things of the future, such as self-driving cars, robotic surgeries, etc.

However, the reality is quite different. Operators are building the network very slowly because they are struggling to find suitable business models that would enable them to sell 5G to the customers while justifying considerable investments that are necessary to start a new technology. With the previous generation (4G or LTE), the business model was clear: fast distribution of a high-quality mobile internet over Czech territory. Furthermore, the government also helped significantly with the distribution of LTE.

With 5G, we see a much more careful approach. Considerable pressure is being placed from the political sphere, which hopes that the network will bring new tech investments into the technological development sphere of Europe. Nevertheless, operators remain careful so far with spending billions for a network when it is unclear which business models will force the customers to buy and use it. In Europe, it is in Finland, the United Kingdom, and Switzerland where the process of putting up 5G is the most progressive. However, they use 5G mostly as a substitution for a fixed-line network. It is mostly used in places where it would be too expensive to provide a fast fixed-line network in a house or apartment. This is certainly attractive and a step forward, but it is still far from futuristic technological conveniences that is expected by architects of the European telecommunication policy.

The biggest problem for 5G networks will be finding the correct business model. We often hear about the network being a great thing for the Internet of Things because it enables us to connect many small devices and gather big amounts of data. But a recent study shows that majority of participating companies do not perceive the Internet of Things like this or do not even know about it.

Safety of 5G networks is currently a very important topic.

Even the European Union is now dealing with problems of security with 5G networks. Based on a suggestion from the European Commission from this March, the member states released a report on an appraisal of risks in the area of the cyber security of the fifth-generation networks, supported by the European Union Agency for Cybersecurity (ENISA). It points out the major threats, the most endangered devices, the principal weak points (including technical and other vulnerable points) and many other strategical risks.

The integrity and accessibility of 5G networks will become one of the major security challenges for the European Union, among them, privacy protection for example. The European Union is therefore about to agree on a set of measures to deal with potential risks in the area of cyber security at both internal and European level.

Even the Ministry of Industry and Trade of the Czech Republic has finished its 5G strategy. The focal point of the strategy will be the possibility to influence industrial applications such as Industry 4.0, Smart City, intelligent transportation systems, e-health, e-education, smart agriculture, etc. One of the Czech priorities is to resolve how to support and accelerate the

building of 5G network and how to use 5G network in the area of developing Industry 4.0 and artificial intelligence applications.

Evaluation of the Security Aspects of 5G Network Implementation and Policy Recommendations on Further Procurements

Written by Adéla Klečková

Introduction

The future of modern technologies is being decided today. With virtual industries thriving, the demand for fast, efficient and ubiquitous network access is skyrocketing worldwide. The 5G network - the next mobile network generation - will soon become the backbone of our key data transmission infrastructure for everything from vehicles to power plants – the Internet of Things.

Yet, at the same time, hand-in-hand with these unprecedented technological and business advances, new challenges of privacy protection and technology security are arising. This paper aims to contribute to the public discussion surrounding security aspects of the implementation of the 5G network and, at the same time, offer clear policy recommendations to stakeholders for further procurement.

The added value of this paper lies in the clear and uncluttered manner in which it is written – cutting through much of the jargon typically associated with emerging, new and complex technologies such as 5G. Given this, it is widely accessible and comprehensible for both the general public and key stakeholders, many of whom may lack the necessary technical background by which to fully understand this arena. The paper also offers key and informed arguments emphasising the importance of adequately securing 5G infrastructure and concrete policy recommendations on how to achieve this. The content of this paper is based, in-part, on discussions with a number of experts from private, public and economic sectors, increasing its practical – and policy – relevance and offering a cross-sectoral approach to the phenomenon at hand.

The paper will give all readers a detailed yet succinct account of the 5G network problematic, as it currently stands, and prepares individuals for talking effectively about the topic both publicly and within the policy community.

The paper is divided into five main sections. The first chapter details the nature of telecommunication technologies more broadly, and explains the importance of the 5G network for the future development of key infrastructure, specifically. Here, the main security risks related to digital networks are listed in order of severity, creating a more concrete picture of what is at stake if the security of the 5G network is neglected.

One of the most active companies in the development of 5G technologies is the Chinese technology giant Huawei. The second chapter will therefore focus on Huawei's adeptness at building 5G infrastructure within the EU and the political and economic ramifications therein. This chapter will also explore the legal tools Chinese government uses to enforce cooperation on individuals as well as companies operating under Chinese jurisdiction.

In order to provide evidence of the potential for – and actual instances of – toxic connections between Huawei and Chinese government, several examples of malicious influence, interference and other insidious operations are explored in more depth in Chapter Examples

of operations of Huawei in its partner countries. These cases include: attempts of espionage in Poland, diplomatic pressure on the Czech Prime minister after banning the Huawei devices from the government offices and hacking and data leakage from the African Union Headquarters in Addis Ababa.

Based on analysis of best practices implemented in several EU member states, as well as drawing on expertise from IT and foreign policy experts, Chapter 4 of the paper then goes on to summarize and offer several security measures that should not be neglected or omitted when implementing the 5G network.

To prepare liberal stakeholders for public appearances, and in order to help them to make the case for the importance of defence and security in terms of 5G network implementation easier, the final chapter of this paper offers three key arguments in support of this initiative: i) price, ii) the risks connected with granting access to key infrastructures and iii) the advantageous position of technology providers)such as Huawei).

About 5G Technologies

In 2016, approximately 10 Zettabytes[1] [of data storage] 'existed' worldwide. Currently, we are at the overall capacity of 30 – 35 Zettabytes of data, and it is expected that this number will double by the middle of 2020.[2] The current data transmission infrastructure, the so-called '4th generation' 4G network is no longer sufficient for the needs of modern technologies, or for the unprecedented increase of data people and machines demand and generate on a daily basis. It is now not a question of whether we need a 5G network, but how quickly we can build one.

So what is 5G? How does it differ from 4G? And why should we be interested in its implementation within critical infrastructure in our nation states?

The development of the telecommunications infrastructure began in the 1980s with a first generation analogue network. The second generation network revolutionized telecommunications infrastructure, bringing with it the transition from analogue to digital. The development of the third and fourth generation networks was then an incremental evolution of this already functioning and widespread technology.

Cellular network: a network made up of individual cells, allowing the user working in such a network without the need for manual switching and selection of individual transmitters.

While the transition from the first to the second generation network is considered to be a major technological 'revolution', the current transition from fourth to fifth generations brings equally significant change. It will allow for the massive expansion in use and capabilities of smart devices that are able to communicate directly with each other (almost) without a human factor behind such a process.

The fifth generation network brings two main advantages. The main technological advantage lies in the enabling of a significantly higher number of devices to be connected to a single cell.

[1] 1 Zettabyte equivalent to 1 billion terabytes

[2] IDC: Expect 175 zettabytes of data worldwide by 2025, https://www.networkworld.com/article/3325397/idc-expect-175-zettabytes-of-data-worldwide-by-2025.html

Some studies suggest 100 times increase compared to the 4G network.[3] A frequency related advantage means that the network will be transmitting in millimeter waves, i.e. at significantly higher frequencies than the existing infrastructure. Higher frequency allows more data to be transmitted.[4] As a result, a 5G network will allow more devices to be connected while transmitting more data.

In many ways, the development of the 5G network is the 'behind-the-scenes' answer to the unrelenting production of ever-innovative smart technologies. The amount of data transferred, as well as the actual number of devices connected to the network is constantly growing. At a time when the average person now needs to connect at least two to three devices, a computer, a phone and possibly a tablet, it is clear that the network parameters of previous generations are no longer sufficient.

Indeed, the amount of connected devices and the volume of data generated is still increasing with a geometric row. Estimates put the actual number of devices at 75 billion by 2025.[5]4G will not be sufficient for such a load. As smart technologies that communicate with each other and form the so-called Internet of Things continues to grow, the development and implementation of a new network that will allow the transmission of such massive data volumes is an inevitable necessity.

Internet of Things: an integrated system of networked devices that allows devices to exchange information and communicate without the need for direct human input.

Smart Critical Infrastructure

The 5G network will allow for a massive expansion of technologies that will – (almost) independently of a human factor – be able to communicate with one another. That is why they are called 'smart'. Such devices spontaneously collect data, send it over the network, and automatically make certain decisions based on them.

The transition to smart technology will affect key civic infrastructure such as transportation, energy, agriculture, manufacturing, health, defence and other sectors. The 5G network will provide a platform for data transfer and communication between all the devices included in the infrastructure.

3 attributes of information security:

- ***confidentiality - data is protected***
- ***availability - data is available***
- ***integrity - data is unchanged***

The complexity and high-paced nature of 5G development creates a number of security risks. Automated communication is more sensitive to data integrity. Decisions are taken

[3] We're building our network to deliver the full potential of 5G. Are you ready?, https://www.verizonwireless.com/business/articles/business/5g-network-performance-attributes/

[4] The disadvantage, however, is that this type of frequency is harder to spread because it can be more easily stopped by physical obstacles. The solution is to increase the number of BTS transmitters to cover the same space.

[5] 80 IoT Statistics (Infographic), https://safeatlast.co/blog/iot-statistics/

automatically based on source data. Any change in the source data may cause wrong decisions being made without the corrective human factor involved. Smart devices can be controlled remotely and by breaching into communication infrastructure, an attacker can cause a traffic collapse, disconnect power to hospitals or even derail a train. Protecting and increasing the resilience of the 5G network technology, which parts of critical infrastructure will be dependent on, is therefore a serious matter of national security and the protection of human life.[6]

Security risks associated with digital networks

The main security risks associated with inadequate network protection include the leakage of (sensitive) data, network decommissioning and access to key network structure information by potentially hostile actors. It is not so much that the same risks were not associated with previous generations of data networks, but that 5G will enable more devices including parts of critical infrastructure to be digitalized and connected to the network which logically increases the potential impact of disruptions or outage, whether man-made or not.

Firmware: a software subcategory used for less "smart" devices.

It is relatively easy for technology manufacturers to write a so-called 'backdoor' in a device's firmware. Of course, such backdoors can be detected, but it is important to keep in mind that the firmware needs to be continuously updated in order to do so. This is a process which in itself increases the chance of human or technological failure, through the potential installment of a compromised operation system, undermining the networks integrity.

Backdoor: A backdoor allows you to bypass the device's protection system and access its data.

At that moment an attacker can gain access to the network, and the entirety of its data is at the attacker's disposal. Such data may include sensitive information leading to potential distortion of state security, but it might also include seemingly unimportant data such as photos or general personal information. However, this data too can be of great value to private companies when creating personalized ads, or for making machine learning more precise. At a time when data is considered the world's most valuable commodity, there is no such thing as 'useless' data.

Another possible risk is a Denial of Service Attack (DOS). As the 5G networks could be at some point in the future connected to critical infrastructure - including energy, electricity, water and transport systems - the failure of its operation may have critical implications for the safety and lives of citizens.[7] Hence, it is in the best interest of all of us that our phones, smart cars or power plants are connected to a network that is reliable and well protected from external attacks.

Denial of Service Attack: a type of cyber attack aimed at shutting down the network, resulting in disruption to the key services that the network provides.

[6] Prague 5G Security Conference announced series of recommendations: The Prague Proposals, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

[7] EU Coordinated Risk Assesment Of the Cybersecurity of the 5G Network (page 5 and 32)

If we allow foreign, potentially hostile actors to build network infrastructure in the first instance, we also risk giving such actors access to the knowledge of the complete topography of such a sensitive data network further down the line. A potential attacker will have a very clear idea of where the bottlenecks of the net to attack are located.

Estonia as a deterrent case: In 2007, Russia used detailed knowledge of the Estonian technological backbone to attempt a coup d'état. The Russian cyber invaders knew where important nodes were located, which made them able to decommission a significant portion of Estonia's infrastructure for several days with simple DDOS (Distributed Denial of Service) attacks. Knowing the weaknesses of the target, the attacker was able to do enormous damage with little effort.

Access to such critical information should only be given to technology providers who are either completely independent of the state or, failing that, come from allied countries. On a purely technical level, if complex monitoring and security mechanisms are implemented throughout the infrastructure building process, then theoretically it could be possible to allow any country to build the telecommunication network. However, this must be reflected in the country's foreign policy strategy. The government of the state must take into account that action taken against the host country will trigger reciprocal action precisely in the form of misuse of knowledge of sensitive infrastructure and be properly prepared for this scenario.

About Huawei and its Relations to the Chinese State

China has made a top-down national pledge and commitment to become a world leader in 5G development and it is very likely to emerge as a front-runner in the technology, with the Chinese expecting 5G to be commercialized globally by 2020. This seems likely, given that the government has recently approved investment of up to $223 billion USD in 5G networks over the course of 2020-2025.[8]

Committing early to the standardization process would give Beijing an additional edge by which to gain influence internationally and generate notable economic impact domestically - not necessarily good news for European Partners. The Chinese national champion for the actual implementation of the global 5G ambitions of the Chinese government are two technological giants: ZTE and Huawei. Because Huawei is very likely to be assigned to the construction of the 5G network in Europe - and, as a result has received the most global attention - this paper will focus primarily on this company.[9]

[8] China to invest $134-223 billion in 5G networks during 2020-2025: Report, https://www.rcrwireless.com/20190312/5g/china-invest-134-223-billion-5g-network-during-2020-2025-report

[9] EU hints at Huawei risk in 5G security assessment, https://www.euractiv.com/section/5g/news/eu-hints-at-huawei-risk-in-5g-security-assessment/

Huawei: a major global technology company and one of the oldest Chinese "private" companies providing information and communication technology infrastructure and smart devices. Huawei holds the second position in the worldwide smartphone market after Samsung (pushing ahead of Apple in 2018). In the delivery of mobile network equipment, Huawei is the world leader just ahead of the Swedish firm Ericsson. Huawei belongs to companies that own several patents on 5G technology.

The divergence between the national states in approach to Huawei is not (solely) driven by different technical interpretations, but comes from fundamentally distinct views about the threat posed by the Chinese Communist Party. In China, that public-private relationship is particularly close-knit because of Beijing's sway in almost every sector of the economy. Huawei is therefore one of many companies, with national and global ambitions, which has close ties and a degree of loyalty to the CPC. Huawei was founded in 1987 by Ren Zhengfei, the former People's Liberation Army officer as a part of CPC's strategy to update outdated telecommunication infrastructure. In order to do so, Ren received a $5.8 million USD loan from the state bank, although the company denies this.[10]

Huawei began its existence by selling imported private branch exchanges. At the same time, Ren examined the imported exchanges through reverse engineering in order to start producing his own copies efficiently and effectively. In the 1990s, Ren sold them to his former employer, the Chinese People's Liberation Army, and the Beijing government began to adopt a policy of supporting its own manufacturers in telecommunications instead of reliance on foreign suppliers. Today, Huawei remains a major vendor for the Chinese state apparatus.

Ties to the Chinese military and intelligence

Over the past decade, Huawei workers have teamed-up with members of various organs of the People's Liberation Army on at least 10 research endeavors, spanning from artificial intelligence to radio communications. This has included a joint effort with the Central Military Commission (the Chinese armed forces supreme body) to extract and classify emotions in online video comments, and an initiative exploring new ways of collecting and analyzing satellite images and geographical coordinates together with the National University of Defence Technology, Changsha.[11]

Such projects are thought to be only a few of the publicly disclosed cases that shed light on how staff at Huawei have teamed with the People's Liberation Army on research into an array of potential military and security applications.

New research analyzing the resumes of Huawei employees further suggests links between the company and the Chinese military and intelligence agencies run deeper than publicly acknowledged. Taking a subset of some 65,000 resumes, researchers have found roughly 25,000 belonging to current or former Huawei employees.[12] The researchers then searched for

[10] Komentář Michala Valáška: Proč je a má být z Huaweie otloukánek, https://archiv.ihned.cz/c1-66526810-proc-je-a-ma-byt-z-huaweie-otloukanek

[11] Huawei Personnel Worked With China's Military on Research Projects, https://www.bloomberg.com/news/articles/2019-06-27/huawei-personnel-worked-with-china-military-on-research-projects

[12] Researchers studied 25,000 leaked Huawei resumes and found troubling links to the government and spies, https://www.businessinsider.com/huawei-study-finds-connections-between-staff-and-chinese-intelligence-2019-7

key terms, such as the People's Liberation Army. From this, they narrowed down the list to just over 100 individuals who had experience in national security.

Besides the close ties between Huawei and Chinese political elites, there is one more reason why the company should be interpreted as a tool of Beijing's geopolitical ambitions. And that is the rather controversial 'National Intelligence Law'. On the other hand, it should be noted, the new laws only legalize previously well-established practices.

A top of that, former long-term CEO of the company Sun Yafang worked for the Ministry of State Security (KGB-like organization) prior to her work at Huawei. [13]

Legislation tools to enforce cooperation

In 2017, the Chinese government passed the National Intelligence Law which includes specifically Article 7: "All organizations and citizens shall, according to the law, provide support and assistance to and cooperate with the State intelligence work, and keep secret the State intelligence work that they know."

Originally proposed as a 'defensive' form of legislation (National Security Act 2015, Counterterrorism 2015, Spy 2016 and Anti-Spy 2014, Cyber Security Act 2016 and Foreign NGO Act 2016), it has in fact become more 'offensive' in scope-and-scale, whereby not only Chinese but also foreign entities, together with individuals, are required to cooperate with the Chinese Secret Services. Data generated by people or entities under Chinese jurisdiction is also considered a critical infrastructure, and the government reserves the right to further use it any way it sees fit. The overarching purpose of the legislation is to control the entire network and its content. It allows access to the facility and databases, investigating personnel, wiretapping and seizing the facility.

Although Huawei itself rejects all allegations and claims that the Chinese law allows the use of the company as a tool for espionage and for the acquisition of sensitive data, and even tries to fool the public by using biased invalid legal opinions, the law speaks clearly. This article legally binds every Chinese company - including Huawei - to provide the Chinese government any information that they require. Thus, taking into account the close connections between the company and the Communist Party[14] more generally, it would be short sighted to simply take Huawei's proclamation of innocence at face value.

Examples of operations of Huawei in its partner countries

Construction of the 5G network gives the vendor unique access to the critical infrastructure of the country. It should therefore be of primary concern to each and every government in granting such an easily abusible knowledge, even in the case of supposedly 'trustworthy' partners. The close connections between the Huawei, the Chinese state, its intelligence services and its military, must only serve to increase this concern.

Monitoring the activities of Huawei abroad is essential for several reasons. First of all, it is astonishing how closely-related, in appearance at least, some of the malicious practices employed by the company are to those of the Chinese intelligence toolkit. Studying Huawei can, in its own way, provide a deeper insight into Chinese operations more broadly.

---

[13] Huawei's Former CEO Worked for China's Spy Agency, Current Exec Admits, https://www.theepochtimes.com/huaweis-former-ceo-worked-for-chinas-spy-agency-current-exec-admits_2959597.html

[14] That plays an important role even in the company's branches abroad through OECs, the renamed Party cells.

Chinese Operations Toolkit:

- ***'playing the man' - focusing on the individual using subtle manipulation (playing to the ego, elicitation, switching between dominance and deference, and controlling the tone and tempo of conversations) with the goal of shaping the personal context***
- ***'service facilitated operations' - intelligence services facilitate meetings and contacts rather than handling the dirty work of influencing foreign targets themselves***
- ***'influenced agents' - gatekeepers who facilitate inroads and make connections in order to open the door for foreigners in China are more common than intelligence officers***

Indeed, mapping Huawei business-practices abroad brings us again repeat empirical evidence of the close connections between the company and the Chinese state. A fact emphasised even more given that the Chinese government has never hesitated to employ any tools available to it (including diplomatic pressure or rest of other countries citizens) in order to put pressure on international actors threatening the business interests of Huawei.

Espionage attempts in Poland

Poland is the second country, after Canada, in which the state authorities have detained someone linked to Huawei under accusation of espionage. This has proven to be an especially bitter pill for Huawei to swallow since it has worked in Poland since 2004, and in 2008 set up its Central, Eastern and Nordic European regional headquarters in Warsaw.

The first to be arrested was Chinese citizen Wang Weijing, a Huawei employee and a former high-ranking Chinese consulate representative in Gdansk. The second was a Polish citizen Piotr D., an employee of the telecommunications company 'Orange Polska SA' and a former Polish security services worker. Evidence suggests that both men committed espionage activities against Poland, in collusion with one another. In response, Huawei released a statement distancing itself from Weijing W., saying his alleged actions have no relation to the company. [15]

Beijing threatened to set off retaliatory measures against Warsaw in light of the arrests. And, just as in the case of the Czech Prime minister (detailed below), the Chinese Embassy was employed as the main tool of public pressure within Poland. The Chinese ambassador to Poland outlined in his interview with the Chinese Global Times the effects that the exclusion of Huawei from the 5G project in Poland will have on Poland's economy. The ambassador estimated the impact on the Polish economy to be in excess of €8.5 billion, that the cost of communication services for ordinary people will more than double, and it will also delay the construction process of 5G network in the country by two to three years.[16]

[15] Poland calls for 'joint' EU-Nato stance on Huawei after spying arrest, https://www.theguardian.com/world/2019/jan/12/huawei-sacks-chinese-worker-accused-of-spying-in-poland-wang-weijing

[16] Huawei, 5G, and China as a Security Threat, https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/

Pressure from Chinese Embassy on the Czech Prime minister

In late 2018, after passing a new law to strengthen its competencies, The Czech National Cyber and Information Security Authority (NCISA) issued a warning of the use of Huawei and ZTE technologies. As a response to this warning and empowered by new legislation, the Czech Prime minister Andrej Babis decided to impose a ban on the usage of Huawei origin devices in governmental offices.

Subsequently, upon the Chinese Embassy's request, a meeting between the Prime Minister and Chinese Ambassador Zhang Jianmin took place. Later the Chinese envoy released a misleading summary of the meeting with the intention of manipulating public perceptions against the PM and in favour of Huawei. However, this attempt was debunked soon enough and the office of the Prime Minister issued an official request for the Chinese Embassy to withdraw the statement. [17]

This seemingly innocuous case nevertheless serves as a prime example of the close cooperation between Huawei and the Chinese Politburo - with Beijing not hesitating to employ diplomatic pressure when the interests of the company are at stake.

Kompro files in the Czech Republic

The investigative team of Czech Radio Radiožurnál published information of the Czech branch of Huawei gathering compromising materials on its business partners and employees, especially those in high-level management positions.

In addition to gathering business information, employees had to record details of personal sensitivity into the internal system. For example, how many children a particular customer has, what his / her private interests are, or how well he / she is doing financially. In addition, it was well-established practice that this information was discussed at internal meetings with people from the Chinese embassy.

Other tasks of the employees of the Czech branch included obtaining personal information about high-ranking state officials, which the company then invited to conferences or trips to China. Simultaneously, Chinese Huawei headquarters also had access to the database containing all the above specified information.[18]

Czech secret services confirmed that they were aware of the practices that Huawei employs, and has described them as “unusual” for business negotiations.

Similar techniques are typical for autocratic regimes working abroad, whereby information is often collected and collated with a clear agenda in mind: to use them as a tool of manipulation or blackmail against the potential targeted stakeholders. Even though they cannot necessarily be seen to be used directly against the targets, mentioning its existence can often serve as sufficient leverage.

Data Leakage in Addis Ababa

Huawei, together with the second state dependent company ZTE have built the majority of Africa’s telecommunication infrastructure (McKinsey Report). Huawei are also the main

[17] Babiš: Nevím, o čem čínský velvyslanec mluví. Vláda chybu neudělala, varování ohledně Huawei bereme vážně, https://www.irozhlas.cz/zpravy-domov/andrej-babis-huawei-cinsky-velvyslanec_1812271050_ogo

[18] Počet dětí, zájmy, majetek. Český Huawei podle exmanažerů řeší klienty s lidmi z čínské ambasády, https://www.irozhlas.cz/zpravy-domov/kauza-huawei-cina-spionaz-citlive-udaje-klientu-cesty-do-zahranici-gdpr_1907220600_per

suppliers of information and communication technology systems to the African Union Headquarters in Addis Ababa, Ethiopia. In January 2018, African mutation of the daily Le Monde reported that the African Union's computer systems had been compromised.

For five years, since January 2012 when the building was inaugurated, the data from the African Union Headquarters had been transferred to servers in Shanghai. The transfer activity was peaking over night on a regular basis - from midnight to 2am - when the offices were expected to be deserted. It was also reported that microphones and listening devices had been discovered in the walls and desks of the building.

Huawei strongly denies being involved or responsible for the data leakage. However according to Danielle Cave of the Australian Strategic Policy Institute it is highly unusual for the supplier of the equipment and key ICT services to remain completely unaware of the apparent theft of a large amounts of data every day for five years.[19]

In reaction, African Union officials have accused China of hacking its headquarters. The situation is especially problematic, since, as they have admitted, African countries have little to no leverage over China. The hack underscores the risk African nations take in allowing Chinese technology companies such prominent roles in developing their telecommunication backbones.[20]

Best prevention practices and further policy recommendations

The purpose of this paper goes beyond simply descriptive analysis of the previous and current potentially problematic 5G situation. In order to move beyond solely accounting for issues which should be cause for concern of policymakers and stakeholders, this paper will now turn its attention to highlighting a number of concrete policy recommendations in order to mitigate the potential risks and increase the security of the telecommunication network. not just to raise the alarm but to also provide a more constructive approach to implementation of the 5G technology as a part of the critical infrastructure of the national states.

These recommendations are arrived at via a number of different sources. Some are derived from official sources such as the cyber security strategies of national states and risk assessments conducted by EU institutions, such as the European Commission and the European Agency for Cyber Security. Other recommendations are based on non-state sources such as academic research, think-tank analysis or discussions with IT and security experts.

There are three main approaches (European) governments have employed regarding Huawei and 5G networks. The first is a complete ban on Huawei 5G operations as may occur in Poland[21] and Sweden[22]. The second is to ignore the risk altogether; an which is is close to the approach taken by Italy which is very opened to involvement of Huawei and fellow Chinese company ZTE Corp in the development of its 5G networks.[23] Hungary have adopted a similarly passive

[19] Huawei: The story of a controversial company, https://www.bbc.co.uk/news/resources/idt-sh/Huawei

[20] African Union accuses China of hacking headquarters, https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5

[21] US and Poland sign 5G security agreement as part of effort to block Chinese telecoms giant Huawei from European networks, https://www.scmp.com/news/china/diplomacy/article/3025419/us-and-poland-sign-5g-security-agreement-part-effort-block

[22] Stopp för kinesisk 5G möjligt med ny svensk lag, https://www.svt.se/nyheter/vetenskap/stopp-for-kinesisk-5g-mojligt-med-ny-svensk-lag

[23] Huawei to invest $3.1 billion in Italy but calls for fair policy on 5G: country CEO, https://www.reuters.com/article/us-huawei-italy/huawei-to-invest-31-billion-in-italy-but-calls-for-fair-policy-on-5g-country-ceo-idUSKCN1UA11V

approach with PM Viktor Orbán stating that he has no evidence of security threats from Huawei equipment. [24]

Last, but definitely not least, governments can attempt to mitigate the possible (and in some cases, probable) risks associated with Huawei and the 5G network, by employing a mix of legal and technical prevention and monitoring tools. A shining example of this approach is the United Kingdom which has developed a comprehensive system to account for the security risks posed by Huawei, by keeping the company out of critical networks and by setting up an evaluation centre to test Huawei equipment. Germany has recently followed suit, announcing the adoption of certification and monitoring schemes towards Huawei activities. These different national assessments of Huawei are to some extent reflected by the various bilateral ties and diplomatic stances of each state towards China. For the duration of this paper, the primarily focus will be on recommendations relevant for nation states which decide to take the third approach.

It is important to state however, that these recommendations are not necessarily aimed at targeting Chinese companies specifically, despite the fact that they currently pose the biggest risk compared to other competitors. Indeed, the applicability of the following recommendations are intended to be universal; a series of remedies to increase the security of a nation state's telecommunication infrastructure.

Recommendations on the operators

Operators of communication infrastructure often depend on technology from other suppliers. Major security risks emanate from the cross-border complexities of an increasingly global supply chain which provides ICT equipment. Over-dependence on a single supplier increases exposure to a potential supply interruption resulting, for instance, from commercial failures, and their consequences. It also aggravates other potential weaknesses and vulnerabilities, increasing the likelihood of their possible exploitation by threat actors, in particular where the dependency concerns a supplier presenting a high degree of risk.[25]

In order to mitigate part of the technical – as well as geopolitical – security risks relating to single supplier dependency, **diversification of vendors** is strongly recommended. Luckily, European network operators usually have multi vendor strategies in place and, despite the obvious financial burden, this precaution should be maintained.[26] Governments need to incentivize telecommunication operators to avoid relying solely on one vendor, encouraging diversification of telecommunication infrastructure by 5G networks with technologies from different companies. This strategy combined with very strict monitoring precautions would, to some extent, decrease some of the security risks connected to the deployment of Huawei technologies.[27]

[24] Huawei to invest $3.1 billion in Italy but calls for fair policy on 5G: country CEO, https://www.reuters.com/article/us-huawei-italy/huawei-to-invest-31-billion-in-italy-but-calls-for-fair-policy-on-5g-country-ceo-idUSKCN1UA11V

[25] EU coordinated risk assessment of the cybersecurity of 5G networks

[26] The Future of Huawei in Europe, http://www.chinafile.com/conversation/future-of-huawei-europe

[27] EU states warn of political risks from 5G suppliers, https://www.ft.com/content/90d53db6-ea7f-11e9-a240-3b065ef5fc55

Network redundancy: a process by which additional or alternative network devices, equipment and communication mediums are installed within network infrastructure. It is a method for ensuring network availability in case of a network device or path failure and unavailability.

Security comes with a price - making more secure devices and operation systems more pricey. On the other hand, Chinese companies sell their already cheaper, lower quality technologies[28] for dumping prices which makes them purely from the financial perspective for many attractive vendors.[29] In order to encourage telecommunication companies to use technologies from reliable vendors - and to partially compensate the higher prices of secure equipment in comparison - national governments should offer tax reliefs and other forms of **financial incentives.**

Recommendation on the technology vendors

Before letting the vendor to built part of critical infrastructure, governments should get to know the company better. Hence a **risk assessment of the supplier** should become an integral part of the selection procedure, and should include an assessment of the legal environment and suppliers ecosystem, and involve participation in multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, and data protection.[30]

This requires identifying potential gaps in existing frameworks and enforcement mechanisms, ranging from the implementation of cybersecurity legislation, the supervisory role of public authorities, and the respective obligations and liabilities of operators and suppliers. This may include assessing the likelihood of suppliers being subject to interference from non-EU countries. Such interference may be spotted by looking for factors such as "strong links" between the company and government, and a government's ability to put pressure on domestic "legislation, especially where there are no legislative or democratic checks and balances in place.[31]"

Excluding all potentially hostile government controlled companies from public tenders would be reasonable. However, if such a blanketed-approach cannot be implemented, it would be wise to at least have a thorough background check on the vendor so that national cybernetic strategies can be adjusted accordingly.

For political, economic and security reasons, the optimal scenario includes one of the **European service providers** to be part of 5G implementation. Unfortunately, the cost factor will continue to impede small service providers – and smaller EU member states - in the

[28] UK Blames 'Defects' in Huawei Tech on Bad Design, Not Spies, https://www.pcmag.com/news/367481/uk-blames-defects-in-huawei-tech-on-bad-design-not-spies
[29] Huawei není transparentní, má dumpingové ceny a poslouchá Peking, tvrdí experti. Firma to odmítá, https://hlidacipes.org/huawei-neni-transparentni-ma-dumpingove-ceny-a-posloucha-peking-tvrdi-experti-firma-to-odmita/
[30] Prague 5G Security Conference announced series of recommendations: The Prague Proposals, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/
[31] EU Coordinated Risk Assesment Of the Cybersecurity of the 5G Network (page 22)

highly fragmented and heavily regulated European telecoms market, from resisting the allure of cheaper Chinese equipment[32] in some instances.

Nontheless, a push for the national (or, in this case, continental) champions – namely Finnish Nokia and Swedish Ericsson – should rank among the best interests of every single EU member state.[33] This should be considered a top priority when deciding the vendors of the 5G networks.[34]

Technical recommendations

Stakeholders should **regularly conduct vulnerability assessments and risk mitigation** regarding all components and network systems, prior to product release and during system operation. Furthermore, they should promote a culture of find/fix/patch to mitigate already identified vulnerabilities and rapidly deploy fixes or patches to emerging weaknesses.[35]

> ***Data encryption: a security method whereby information is encoded and can only be accessed or decrypted by a user with the correct encryption key. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing it without permission.***

Among measures to prevent the penetration of systems or the installation of compromised operation systems within the infrastructure, some best practices already exist, at least partially. These concern in particular, security requirements applicable to previous generations of mobile networks, which for the time being at least remain appropriate for the future deployment of 5G networks. For instance; technical measures (e.g. multi-level encryption, authentication, automation, anomaly detection) and process-related measures (e.g. vulnerability management, incident and response planning, user-privilege management, disaster recovery planning).[36]

> ***Monitoring in the UK: The Huawei Cyber Security Evaluation Center (HCSEC) - an Oxford-based joint center, staffed by Huawei-employed technicians and overseen by the National Cyber Security Center (NCSC) as well as Government Communications Headquarters (GCHQ) - was established in 2010 to test whether or not Huawei products have any flaws or backdoors.***

[32] Exclusive: EU cites Chinese telecoms Huawei and ZTE for trade violations, https://uk.reuters.com/article/us-trade-eu/exclusive-eu-cites-chinese-telecoms-huawei-and-zte-for-trade-violations-idUSBRE94H03J20130518

[33] Europe should heed this wake-up call regarding 5G, https://www.businesstimes.com.sg/opinion/europe-should-heed-this-wake-up-call-regarding-5g

[34] The Future of Huawei in Europe, http://www.chinafile.com/conversation/future-of-huawei-europe

[35] Prague proposals: Officials agree 5G security recommendations, https://www.mobileeurope.co.uk/press-wire/prague-proposals-officials-agree-5g-security-recommendations

[36] Prague 5G Security Conference announced series of recommendations: The Prague Proposals, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

However, the fundamental differences in how 5G operates also means that the current security measures as deployed on 4G networks might not be less effective or sufficiently comprehensive to mitigate the identified and emerging security risks associated with 5G.

Recommendations for state officials

Cyber security cannot be regarded as a purely technical issue, but also demands that a number of specific political, economic and societal actors be taken into account. A safe, secure and resilient infrastructure requires adequate national strategies, sound policies, and a comprehensive legal framework with dedicated personnel, who are trained and educated appropriately. Strong cyber security supports the protection of civil liberties and privacy throughout all nation states.

Laws and policies governing networks and connectivity services should therefore be guided by principles of **transparency and equitability**, taking into account the global economy and interoperable rules, with sufficient oversight and respect for the rule of law.

German no spying deal: Berlin published its draft 5G security catalogue, which allows Chinese companies to build 5G critical infrastructure. Huawei and ZTE had to sign a declaration of trustworthiness vis-à-vis the network operators.

When letting a supplier with notable connections to a potentially hostile third country into critical infrastructure, the risks of influence on the supplier by this country.

try should be taken into an account. **The international politics strategy and the cybernetic strategy** of the national country should be amended accordingly. In the case that financial sanctions – or other forms of international penalties – are imposed on a third country, national cyber offices should be prepared for possible outages or for other forms of retaliatory measures.

With more and more critical infrastructure being relocated into the virtual space, competencies of national cybernetic offices should be strengthened accordingly. The growing importance of such institutions within the national security architecture of states suggests already that they will come to play an increasingly crucial role in the not so distant future.

Czech Warning Mechanism: In 2014, the Czech republic introduced a Law on Cybernetic Security which included a warning mechanism, enabling its National Cyber and Information Security Agency (NÚKIB) to issue official warnings against cyber security threats such as malicious technologies, which the Czech Government and other State Institutions are now legally bound to address further and take into account. The first use of this new mechanism was to issue an official warning against Huawei technologies in late 2018.

It is suggested that nation states implement **mechanisms for screening of foreign investments** into their national legislation. Even though this precaution does not tackle risks connected to the implementation of the 5G network directly, it prevents purchase of telecommunication operators by companies linked to a potentially hostile states.

Finally, **sharing experience and best practices**, and **providing appropriate assistance**, with regards to the mitigation, investigation, response and recovery of network attacks, compromises, or disruptions, is crucial if the ambition to building secure and functioning 5G networks across Europe is to be successful.

Appendix: Arguments supporting the emphasis of proper security of the 5G infrastructure

With the intention of increasing the practical added value of this paper, several reaction points supporting the increased emphasis on the security aspect of 5G implementation is included below. These points should serve as solid foundations upon which to refute the main claims and arguments used by those who are uncritically in favour of Huawei providing technologies and building the 5G network.

Primarily, this support tends to centre around its undeniably low price. The Chinese government using Huawei as its tool for malicious influence operations does not appear to put off potential partners, given its profitability through the use of state subsidies. This allows the company to sell its devices for 'dumping' prices.[37]

Two main arguments can be used against this economic argument in favour of Huawei, both showing that the overall price can in fact grow significantly higher than the original one quoted; i) the lower quality of the technology and ii) the need for additional security measures.

This appendix serves as a starting point for public appearances and communication for liberal politicians and other stakeholders.

Lower quality of the technology

Huawei does not only pose a security risk in geopolitical terms, but also technically, given its inferior approach to the security of its devices. A special oversight board that reports to the UK government on the safety of Huawei's devices has found "serious and systematic defects" in the way Huawei engineers its software and practices cybersecurity.[38]

A number of vulnerabilities were found in the networking technologies which, if discovered by attackers, could seriously disrupt telecommunication networks, allow them access to customer traffic or disrupt the technology altogether. The report further says that "the scale and severity of vulnerabilities discovered along with architectural and built issues by the relatively small team is a particular concern."

What is more, such security concerns are nothing new. Huawei has been called on to pay greater attention to such problems for several years. "The Oversight Board currently has not seen anything to give it confidence in Huawei's ability to bring about change via its transformation program," the report adds.

Additional security measures

Together with the objectively low software security of its devices, Huawei technologies can be used as a tool for espionage by the Chinese government, as underlined throughout this paper. Warnings of such kind have been issued by intelligence services across the globe. Hence, Huawei devices should be perceived and treated as risky. [39]

If it becomes inevitable that Huawei will build communication networks, complex monitoring and stringent security criteria need to be implemented effectively in order to make the Chinese technology feasible for deployment into key infrastructure. Among such measures are additional revision mechanisms, double or triple decoding, reverse engineering or other

[37] The Future of Huawei in Europe, http://www.chinafile.com/conversation/future-of-huawei-europe
[38] UK Blames 'Defects' in Huawei Tech on Bad Design, Not Spies, https://www.pcmag.com/news/367481/uk-blames-defects-in-huawei-tech-on-bad-design-not-spies
[39] METODIKA K VAROVÁNÍ ZE DNE 17. PROSINCE 2018, https://www.govcert.cz/download/kii-vis/2019_01_04_metodika_k_varov%C3%A1n%C3%AD_z_17-12-2018_v1.0.pdf

methods of increased monitoring. All of these additional security measures are not cheap, which can make the final costs of deployment of Chinese technologies significantly more pricey than originally quoted.

Ultimately, the choice comes down to more expensive – yet more trustworthy and secure devices in the first instance, or initially cheaper but less secure (and in the end more expensive) devices further down the line. As suggested in the Prague Recommendations, government's should strongly consider the merits of the former, even if the initial cost seems appealing.[40]

[40] Achieving a proper level of security sometimes does require higher costs. Increased costs should be tolerated if security necessitates it.

Case study: Fake news & 5G on the Czech internet

Written by Roman Máca

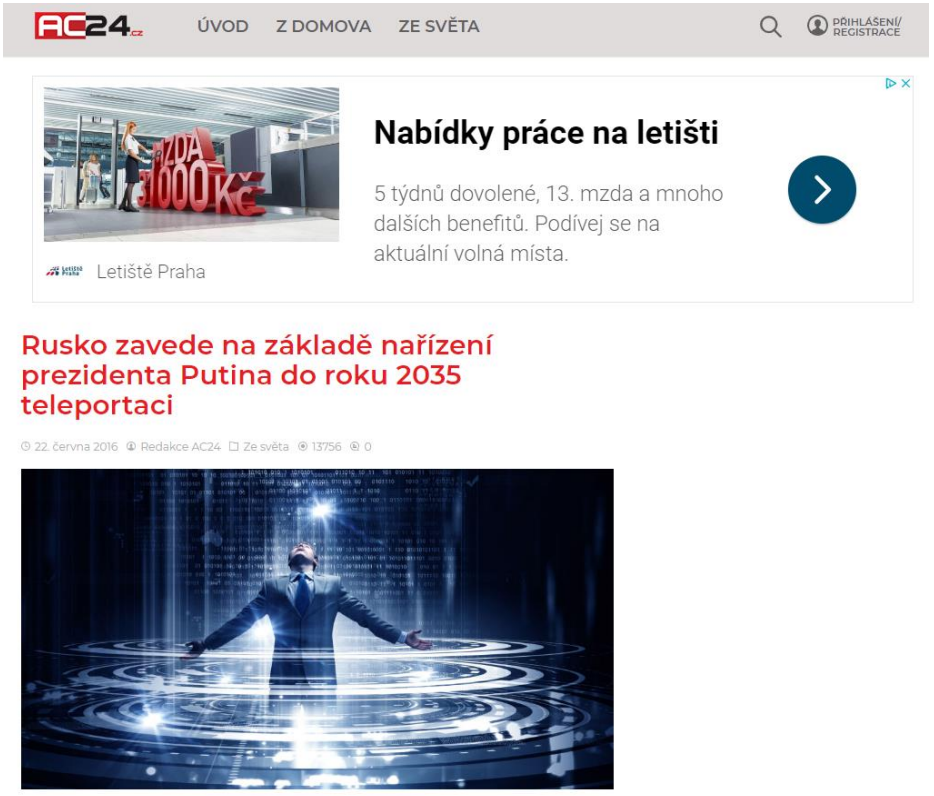
5G is a new telecommunication standard. 5G has been implemented around the world as well as in the Czech Republic. This 5G topic is also getting into the media and into the agenda of fake news websites. This case study has an ambition to describe how 5G is presented and framed by the Czech disinformation scene. There was a sample of articles taken from the website AC24.cz[41], one of the most popular fake news websites in the Czech Republic. The study also presents potential risks and threats as well as recommendations, how to decrease or eliminate negative side-effects.

Nowadays, the operators receive calls from municipalities where 5G is or should be implemented. The municipalities are facing many questions from citizens that are worried about their health. The questions are linked to the articles on fake news websites.

Research sample and particular articles

There were observed (on 23 October 2019) 31 articles including the term „5G“ on the AC24.cz website. The first article was published on 22 June 2016 (the website was established in 2011). The article has title: **“Russia, on Putin’s command, will implement teleportation in 2035.”**

Figure 1: Article preview “Russia, on Putin’s command, will implement teleportation in 2035”



Source: AC24.cz

[41] Founded in 2011 by entrepreneur Ondřej Geršl. The website regularly shares Russian state propaganda and various conspiracy theories. More about the AC24.cz you can find in the last chapter.

The article originates from Russian state propaganda outlet Sputnik. There, 5G is described as a part of the Russian program "National Technologic Initiative". The final phase of the program is teleportation.

There were 3 articles published with the term "5G" in 2016. From the table below it is visible the 5G topic became popular for AC24.cz in 2019. Since 2019, 5G has been implemented in the Czech Republic.

Table 1: Annual quantity of articles with the term „5G"

2016	3
2017	2
2018	1
2019 (till 23. 10.)	25

Source of data: AC24.cz

AC24.cz shows in every article an interesting indicator – number of views.

Table 2: Top ten articles including the term „5G" (translated from Czech)

Headline	**Number of views**
With 5G we will launch the war against humanity! A strong warning to the high representatives of the UN	543 753
Disclosure: 5G is an offensive weapon determined to destroy humanity. Inform yourself!	102 918
Dead bees, birds and dying trees. These are the first impacts where 5G has been implemented	93 887
5G has been coming. A journalist worried about his own health was silenced. What can 5G cause?	55 999
Invisible destruction: Vienna is a warning how 5G networks can damage health	35 893
Experts warn against 5G radiation. It is already used as a weapon in demonstrations. Is humanity the next victim?	33 892
Another warning before effects of 5G network take hold. 215 scientists published a call to stop this activity!	29 066
Danger is hiding in 5G networks. Expert presented shocking facts and he won the first trial	25 109
Dead bees falling at 5G transmitters. What impact will this have for the human body?	23 821
Democratic congressman: Russia committed „an act of war" against the USA	17 032

Source of data: AC24.cz (data at 23 October 2019)

With 5G we will launch the war against humanity! A strong warning to the high representatives of the UN

This is the most popular article with 543 753 views. The article was re-printed from another fake news website zvedavec.org.[42]

It is said in the text, "The government and industry are connected to the implementation of 5G. They have no interest in the safety of the public. This technology promises to be very profitable. 5G also forces everyone to be a part of a new established technocracy."

5G, as it is written in the article, will cause: "Lower fertility, neurologic/neuropsychiatric effects, damaging of DNA, death of cells, damaging of free radicals, hormonal effects, problems with calcium balance and cancer."

Disclosure: 5G is an offensive weapon determined to destroy humanity. Inform yourself!

With 102 918 views, this article is on 2nd place. The article is re-printed from the fake news website tadesco.cz.[43]

Part of the text: „If you see the headlines in US media, you will be persuaded that 5G is the amazing next generation of wireless technology, which will make everything faster, easier and more amazing. But that is all a lie, because 5G is really an advanced overcoated military attack weapon realized to be a final solution against humanities freedom."

The article also mentions a movie: "In the film "5G Apocalypse – an eye opening film" you will see the truth about 5G networks in horrible detail. 5G is not only attacking all aspects of peoples lives, but it will also eliminate privacy, and it will be the most dangerous technology to health, which has ever been created."

5G is also mentioned as a technological crime, which exists in opposition to the meaning of life.

Dead bees, birds and dying trees. These are the first impacts where 5G has been implemented

This article has 93 887 views (3rd place). The article is a compilation of videos on YouTube that are trying prove the dangers of 5G.

It is said in the lead paragraph, "There has been many shocking videos from countries around the world, where 5G has been implemented or tested. If 5G technology is the main reason for the deaths, scientists worries will be fully confirmed."

[42] Samples of disinformation on zvedavec.org (in Slovakian) https://www.konspiratori.sk/assets/screenshots/s.php?i=zvedavec.org.png
[43] Samples of disinformation on tadesco.cz (in Slovakian) https://www.konspiratori.sk/assets/screenshots/s.php?i=tadesco.cz.png

Figure 2: Article preview "Dead bees, birds and dying trees. These are the first impacts where 5G has been implemented"

Source: AC24.cz

5G has been coming. A journalist worried about his own health was silenced. What can 5G cause?

This article is in 4th place with 55 999 views. The article was likely translated from foreign resource.

There is mentioned in the lead paragraph, "Earlier it was 3G then 4G and now we are going to the era of 5G. Although they are saying, what an improvement it will be, it brings damaging ultra-high frequencies of microwaves. People who have raised their voices against the danger about what this technology can bring. People spoke about safety and attempts to silence them through threatening and harassment."

Invisible destruction: Vienna is a warning how 5G networks can damage health

This article is in 5th place with 35 893 views. The article is re-printed from the fake news website badatel.net.[44]

The lead paragraph is saying: „The Coming of the 5th generation mobile networks (5G) evidently represents the biggest threat for existence of life on this planet."

This is said in the article, "For example in Austrian Vienna, where 5G was supposedly implemented in very short time, local people are suffering from bloody noses, headache, pain in the eyes, chest, stomach aches, vomiting, tiredness, dizziness and symptoms of flu and heart ache."

[44] Samples of disinformation on badatel.net (in Slovakian) https://www.konspiratori.sk/assets/screenshots/s.php?i=badatel.net.png

The author of the article describes 5G as „a lethal weapon targeting people“.

The reach of the articles

The number of views of all reported 31 articles on AC24.cz is 1 156 565 according to the web data. The complete list of articles (in Czech) including data of publishing, number of views and URL is in the appendix.

The real reach of the shared messages is much higher. AC24.cz is re-printing the content from other resources and other resources are re-printing articles from AC24.cz.

Not mentioned is the impact from social networks where messages such as “Shocking news, 5G is a lethal weapon for killing all of “humanity“ are shared as posts without opening the article. Content like this is also often shared by chain e-mails and other communication tools.

AC24.cz uses mostly Facebook (FB). By their FB pages of contemporary and former projects they are reaching an audience of 120 000. This project also uses “alternative“ FB pages established only to promote AC24.cz content. It is about 20 pages named „I want to know the truth“ (Chci znát pravdu – see below); Czechs and Slovaks support the Russian Crimea; Cancer – alternative treatment and prevention. These pages have tens of thousands of followers.

Figure 3: The article "With 5G we will launch the war against humanity! A strong warning to the high representatives of the UN" posted on the "alternative" FB page established only to promote AC24.cz content.

Source: Facebook.com

There are also fake profiles (mostly of attractive women) for spamming AC24.cz content into many groups on social networks.

The framing of the term "5G" on AC24.cz

If we put together words from observed headlines (31 articles where is „5G mentioned), we get the following wordcloud (in Czech):

Figure 4: Wordcloud made from headlines

Source of data: AC24.cz

The term „USA" is dominating. USA on the Czech fake news websites is a symbol of pure evil in the world. Important terms are dedicated to health issues and consequences for health. There are also mentioned are these terms Russia, China, Huawei which are often portrayed as victims or opponents of the USA.

We can read the „5G" framing (in general) as a following sentence:

Warning: 5G networks coming from the USA are a source of radiation damaging health. 5G is a tool from the USA used against Russia, China and Huawei.

Fake news about 5G as a threat

With the spreading of fake news about 5G, we can indicate particular threats:

- Increased panic of the public.
- Damage of health. Fake news websites often publish recommendations on how to prevent specific diseases. For example, as a prevention from cancer they recommend to drink a disinfectant for swimming pools.
- Damage of the property of operators. People believing 5G is a danger for them are attacking transmitters.
- Pressure on municipalities to stop network construction projects.
- Economic detriment on micro and macro levels.
- Decreasing levels of trust in public institutions and democracy. Citizens believe that the government wants to kill them through 5G.

How to prevent or eliminate threats?

- Investigation if the "news" content is not in accordance with the law.
- Offended operators/organizations should legally defend their actions.
- Organizations should cancel advertising on fake news websites.

Figure 5: Advertisement of T-Mobile on AC24.cz next to the headline "5G has been coming. A journalist worried about his own health was silenced. What can 5G cause?"

Source: AC24.cz

- Responsible authorities should provide quality information for the public. The organizations need quality strategic communication.
- Restrictive steps taken by social media providers towards fake news resources.
- Development of media literacy.[45]

About AC24.cz

One of the most popular commercial fake news websites in the Czech Republic. Established in 2011 by entrepreneur Ondřej Geršl. AC24.cz has a motto, "Alternative news from the world. Information which you cannot get any other place."

AC24.cz published content of Russian state propaganda and other fake news resources. They publish various conspiracy theories about chemtrails, HAARP, 9/11, aliens etc., medical issues, as well as content which can be classified as hate speech.

Conclusion

Fake news surrounding 5G should not be underestimated. A successful digitization and innovation process is essential for further development of Europe.

In the Czech Republic operators get many messages and calls from citizens that are worried about their health. The municipalities responsible for infrastructure building permissions also receive the similar messages from citizens that are calling to stop the implementation of 5G.

The motivation for spreading fake news about 5G is kind of activism, where the people behind it are convinced that 5G means an apocalypse and damage for their health. But there are also activities connected with simple fake news business based on earnings from the advertisement placed on fake news websites – more views means higher income – which is the case of the mentioned platform AC24.cz.

Europe is active in the fields of securing democratic processes and countering disinformation in general. The topic of countering fake news around 5G is another challenge as is, for example, disinformation about vaccination that brings many risks to the public.

[45] According to „STEM Agency" research (June, 2016) 24,5 % of Czechs trust more to „alternative media" such as AC24.cz than traditional media.

Appendix: List of the reported articles (in Czech)

Headline	Date of publication	Number of views	URL
5G spustíme válku proti lidstvu! Silné varování vysoce postaveným členům v OSN	23 March 2019	543753	https://ac24.cz/-/5g-spustime-valku-proti-lidstvu-silne-varovani-vysoce-postavenym-clenum-v-osn
Odhalení, že 5G je útočnou zbraní určenou k ničení lidstva. Informujte se!	25 May 2019	102918	https://ac24.cz/-/odhaleni-ze-5g-je-utocnou-zbrani-urcenou-k-niceni-lidstva-informujte-se-
Mrtvé včely, ptáci a umírající stromy. Takové jsou první důsledky, kde běží 5G	2 August 2019	93887	https://ac24.cz/-/mrtve-vcely-ptaci-a-umirajici-stromy-takove-jsou-prvni-dusledky-kde-bezi-5g
5G přichází. Reportéra, co měl obavy o zdraví, umlčeli. Co může způsobit?	11 June 2017	55999	https://ac24.cz/-/zpravy-ze-sveta/10500-5g-wifi-reporter-umlcen-zdravi
Neviditelná zkáza: Vídeň je výstrahou, jak dokáží 5G sítě zničit zdraví	30 July 2019	35893	https://ac24.cz/-/neviditelna-zkaza-viden-je-vystrahou-jak-dokazi-5g-site-znicit-zdravi
Odborníci varují před 5G zářením. Už teď se používá jako zbraň při demonstracích. Je na řadě lidstvo?	10 July 2019	33892	https://ac24.cz/-/odbornici-varuji-pred-5g-zarenim-uz-ted-se-pouziva-jako-zbran-pri-demonstracich-je-na-rade-lidstvo-
Další varování před účinky sítě 5G. 215 vědců podalo výzvu k zastavení této aktivity!	10. August 2019	29066	https://ac24.cz/-/dalsi-varovani-pred-ucinky-site-5g-215-vedcu-podalo-vyzvu-k-zastaveni-teto-aktivity-
Nebezpečí skrývající se v sítích 5G. Odborník předkládá šokující fakta a vyhrál první soud	24 January 2019	25109	https://ac24.cz/-/nebezpeci-skryvajici-se-v-sitich-5g-odbornik-predklada-sokujici-fakta-a-vyhral-prvni-soud
Padající a mrtvé včely u 5G vysílačů. Jaké to bude mít důsledky pro lidské tělo?	11 September 2019	23821	https://ac24.cz/-/padajici-a-mrtve-vcely-u-5g-vysilacu-jake-to-bude-mit-dusledky-pro-lidske-telo-
Demokratická kongresmanka: Rusko spáchalo proti USA „válečný akt“	21 March 2017	17032	https://ac24.cz/-/zpravy-ze-sveta/10063-demokraticka-kongresmanka-rusko-spachalo-proti-usa-valecny-akt
Škodlivému vysokofrekvenčnímu 5G záření ze satelitů na oběžné dráze neunikne na zemi žádný živý tvor	4 June 2019	16391	https://ac24.cz/-/skodlivemu-vysokofrekvencnimu-5g-zareni-ze-satelitu-na-obezne-draze-neunikne-na-zemi-zadny-zivy-tvor

Soros označil čínského prezidenta za největšího nepřítele otevřené společnosti. Přišla tvrdá reakce čínského ministerstva	25 January 2019	15869	https://ac24.cz/-/soros-oznacil-cinskeho-prezidenta-za-nejvetsiho-nepritele-otevrene-spolecnosti-prisla-tvrda-reakce-cinskeho-ministerstva
Rusko zavede na základě nařízení prezidenta Putina do roku 2035 teleportaci	22 June 2016	13756	https://ac24.cz/-/zpravy-ze-sveta/8242-rusko-zavede-na-zaklade-narizeni-prezidenta-putina-do-roku-2035-teleportaci
Zastavte přípravy na uvedení do provozu 5G mobilních telefonních sítí. Otevřená výzva české vládě	23 July 2019	13382	https://ac24.cz/-/zastavte-pripravy-na-uvedeni-do-provozu-5g-mobilnich-telefonnich-siti-otevrena-vyzva-ceske-vlade
Japonsko upouští od rozvoje 5G sítí kvůli zdraví občanů	23 June 2019	12994	https://ac24.cz/-/japonsko-odpousti-od-rozvoje-5g-siti-kvuli-zdravi-obcanu
Prvních 6 z 600 satelitů úspěšně odstartoval. OneWeb umožní do roku 2027 5G internet pro všechny obyvatele Země	28 February 2019	12823	https://ac24.cz/-/prvnich-6-z-600-satelitu-uspesne-odstartoval-oneweb-umozni-do-roku-2027-5g-internet-pro-vsechny-obyvatele-zeme
Skrytá vlastnost 5G sítě	13 February 2019	12785	https://ac24.cz/-/skryta-vlastnost-5g-site
Zapojíme se do války na Ukrajině: Okamura rozluštil prohlášení ze setkání Babiše s Trumpem	8 march 2019	11445	https://ac24.cz/-/zapojime-se-do-valky-na-ukrajine-okamura-rozlustil-prohlaseni-ze-setkani-babise-s-trumpem
Návštěva Pence ukázala, že USA nejsou spojenci, ale pány Polska!	7 September 2019	9600	https://ac24.cz/-/navstena-pence-ukazala-ze-usa-nejsou-spojenci-ale-pany-polska-
USA popírají, že vytvořily Islámský stát a obviňují Turecko z šíření „falešných zpráv“	30 December 2016	8547	https://ac24.cz/-/zpravy-ze-sveta/9478-usa-popiraji-ze-vytvorily-islamsky-stat-a-obvinuji-turecko-z-sireni-falesnych-zprav
Brusel se stal prvním městem, který zastavil vývoj 5G kvůli neblahým účinkům na zdraví	6 April 2019	8039	https://ac24.cz/-/brusel-se-stal-prvnim-mestem-ktery-zastavil-vyvoj-5g-kvuli-neblahym-ucinkum-na-zdravi
Proč dohoda ruské společnosti MTS a čínského podniku Huawei vylekala USA	13 June 2019	7248	https://ac24.cz/-/proc-dohoda-ruske-spolecnosti-mts-a-cinskeho-podniku-huawei-vylekala-usa
Máme jiné zájmy! Schröder tvrdě odpověděl USA	16 March 2019	7019	https://ac24.cz/-/mame-jine-zajmy-schroder-tvrde-odpovedel-usa
Špičkový výzkumník rakoviny přirovnává bezdrátově záření škodlivostí k azbestu a cigaretám	15 September 2019	6838	https://ac24.cz/-/spickovy-vyzkumnik-rakoviny-prirovnava-bezdratove-zareni-skodlivosti-k-azbestu-a-cigaretam

Známý český novinář pálí ostrými: Ředitel BIS se stává bezpečnostním rizikem pro tento stát	3 October 2019	6502	https://ac24.cz/-/znamy-cesky-novinar-pali-ostrymi-reditel-bis-se-stava-bezpecnostnim-rizikem-pro-tento-stat
Expert: Když bude reakce Číny tvrdší, Američanům mohou přestat létat rakety	2 June 2019	6490	https://ac24.cz/-/expert-kdyz-bude-reakce-ciny-tvrdsi-americanum-mohou-prestat-letat-rakety
„Státy EU se musí kát, než pronášet prázdné sliby bez praktických důsledků," doporučuje Merkelová	10 September 2016	6461	https://ac24.cz/-/zpravy-ze-sveta/8717-eu-kat-merkelova
Má cenu koupit si starší model iPhonu?	28 July 2019	5351	https://ac24.cz/-/ma-cenu-koupit-si-starsi-model-iphonu-
Navzdory ničící kampani. Huawei dobývá světový trh chytrých telefonů	24 January 2019	5306	https://ac24.cz/-/navzdory-nicici-kampani-huawei-dobyva-svetovy-trh-chytrych-telefonu
Obchodí válka USA-Čína, kolaps summitu Kim-Trump, štěpící se frakce uvnitř amerických elit	26 May 2018	5283	https://ac24.cz/-/obchodi-valka-usa-cina-kolaps-summitu-kim-trump-stepici-se-frakce-uvnitr-americkych-elit
Handelsblatt: Velvyslanec USA hrozil Berlínu za spolupráci s Huawei!	14 March 2019	3066	https://ac24.cz/-/handelsblatt-velvyslanec-usa-hrozil-berlinu-za-spolupraci-s-huawei-

Source of data: AC24.cz (data at 23 October 2019)