CAUGHT IN THE MIDDLE: NORTH MACEDONIA'S JOURNEY TO „CLEAN 5G"

CAUGHT IN THE MIDDLE: NORTH MACEDONIA'S JOURNEY TO „CLEAN 5G"

TITLE OF THE PUBLICATION:
Caught in the Middle: North Macedonia's Journey to "Clean 5G"

Author: Bojan Georgievski

PUBLISHER:
ESTIMA – Association for strategy creation, research, education and promotion of international values

Graphic design: In Design Studio

May 2022

The publication has been prepared in the framework of the project
Promoting a values-based approach in the cooperation between North Macedonia and the People's Republic of China

This project was funded through a U.S. Embassy grant. The opinions, findings, and conclusions or recommendations expressed herein are those of the authors and do not necessarily reflect those of the U.S. Government.

EXECUTIVE SUMMARY

This policy brief looks at the implementation of the China-led "Digital Silk Road" (DSR) in the Western Balkans, emphasizing the issue of 5G networks. It specifically focuses on the efforts of North Macedonia, a country in the Western Balkans, to ensure a secure rollout of 5G networks while maintaining collaboration with Chinese companies. The brief sets out to outline whether the actions that the Macedonian Government took, such as joining the US-led Clean Network Initiative, followed by legislative amendments to limit the presence of Chinese companies, were guided by national security motives or were a political measure taken for aligning its strategic priorities with its Western allies. The brief concludes that although true to its EU ambitions, the steps taken by the Government of North Macedonia to ensure a safe 5G rollout seem to be motivated by political factors and not by national security concerns. The brief identifies the critical loopholes in the Law on Electronic Communications and its bylaws that govern risk assessment of telecommunications suppliers that, if left unchecked, might hinder certain communication equipment suppliers and manufacturers operating on the market. The brief concludes that the principles introduced in the relevant legislation deviate from the principles of transparency, legal certainty, nondiscrimination, and proportionality, which are fundamental principles of the EU Treaty. Finally, the policy brief provides recommendations for the Government of North Macedonia, legislators, the EU, and the People's Republic of China, given the possibilities for ensuring a competitive communications sector while staying true to the EU aspirations.

Keywords:

5G, North Macedonia, Clean Network Initiative, Digital Silk Road

THE DIGITAL CONNECTIVITY RACE

China's Belt and Road Initiative (BRI) was launched in 2013 and set out to strike partnerships with countries worldwide on infrastructure projects, financial ventures, and security initiatives. Over time, the BRI has become the primary tool of the Chinese Government's attempts to gain a global leadership role. Some experts[1] point out that Chinese authorities grew disillusioned with the US-led international order and wanted to offer an alternative that would "improve the global governance." Hence, the BRI.

In 2015, the Chinese Government introduced an extension to its Belt and Road Initiative, firstly called the "Information Silk Road" and later rebranded to a catchier name "Digital Silk Road" (DSR)[2]. The purpose of the DSR is to expand the influence of Chinese companies worldwide, with a main focus on global digital connectivity.

China's vision of the DSR includes operating in the sphere of construction of cross-border optical cables, fast (5G) telecommunication services, and other connectivity fields to be implemented between China and the BRI countries[3].

China's efforts led to its presence in more than 150 countries[4] that have supported the DSR in some shape or form in healthcare, environment protection, digital technologies, and road infrastructure[5].

Some critics[6] have said that the DSR is a means for China to establish global (digital) dominance and gain traction in the "digital arms race" with the US and the EU. Indeed, both the European Union and the US have increased their efforts to counter the Chinese efforts to take the lead in the race for digital superiority. In this race, the Western Balkans would have a prominent role.

ENTER THE (TROJAN) DRAGON

The Western Balkans have become an essential aspect for implementing the Chinese DSR[7]. All countries in the Western Balkans (Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, Serbia, and Kosovo) have EU membership aspirations, some of them on the cusp of starting negotiations for entering the European Union.

However, the EU has had a somewhat ambivalent approach to welcoming the Western Balkan countries into the Union due to lingering security and corruption issues plaguing most countries. This has left the door wide open for China to step in and establish a strong presence in some of the Western

Balkan countries (most notably Serbia) and put in (through loans and investments) billions of euros into infrastructure.

Economic considerations come hand in hand with political ones. Penetrating the market in the EU's neighborhood may pave the way for China to exert future strategic influence on socio-political processes in the EU[8]. On the other hand, the EU and the US see the increased presence of China in the Western Balkans as a security threat for the entire Europe[9].

The main concern of the West about the DSR is that as China becomes more assertive on the global stage, it will use the DSR to spread its model of technology-enabled authoritarianism. Ultimately, the fear is that it would undermine personal freedoms and sovereignty in the countries it is doing business with.

Chinese technology companies have already helped some of the governments in the Western Balkans develop surveillance capabilities that could be used for severe violations of individuals' privacy and data protection rights.

One of the projects that Serbia has struck with Huawei has drawn criticism[10] from the civil society in the country. It concerns the Government's plan to install thousands of facial recognition cameras made by Huawei across the country. Critics fear that the technology's (which is banned in the EU) real aim is to target Government opponents, including activists and journalists, and to diminish free speech and dissent in the country.

Serbia has even recently proposed a law that, if adopted, would place it as the first country in Europe that would make indiscriminate surveillance of citizens lawful[11]. Undoubtedly, the implementation of that law would be aided by the facial recognition cameras produced by Huawei.

Such practices have not gone unnoticed, though. The US recognized that China was trying to get a foothold in the "digital arms race" by trying to get a firm foothold in the communications sector in the Western Balkans, especially when related to 5G infrastructure. Therefore, it has led the efforts to negotiate a pathway to a more secure and stable network and communication infrastructure with European countries. An infrastructure that the Chinese presence would not mar. Such efforts have led to introducing the US-led "Clean Network Initiative[12]."

THE CLEAN NETWORK INITIATIVE

The 2020 Clean Network Initiative has been introduced to ensure a "5G Clear Path," meaning no correspondence between the US Embassies would go through "unfiltered" networks or systems. Those systems would not be named, but it is widely implied that the phrasing is meant to convey Chinese telecommunications companies and 5G providers.

The US managed to get the signatures of several Balkan countries that joined the initiative at a moment when 5G was becoming a priority and a main talking point in the region when it comes to improving digital connectivity.

The Clean Network Initiative does not explicitly mention other countries or specific companies. Yet, it is widely believed that it was developed to diminish the strategic reach of Chinese giants such as Huawei and ZTE and slow down their momentum in building 5G infrastructure worldwide. The Initiative was driven by security and espionage concerns and the possibility of China interfering in democratic processes in Western countries.

This approach of the US towards China can be traced back to 2012 when Congress warned that the "United States should view with suspicion the continued penetration of the US telecommunications market by Chinese telecommunications companies[13]."

More recently, their most prominent target would be Huawei, one of the world leaders in 5G technology. Huawei was already a leader in providing 4G networks in several European countries and hoped to secure a large number of the new 5G infrastructure partnerships. However, the US administration took an aggressive[14] stance toward the Chinese tech giant and identified the company as a security threat, echoing espionage or even sabotage concerns. On the other hand, Huawei accused the US of violating international trade rules and said it had no ties to the ruling Chinese Communist Party.

Soon enough, the US would get the support of more than 50 countries and 170 telecommunications companies that "refuse to allow their 5G networks to be compromised by untrusted vendors". North Macedonia is one of them.

NORTH MACEDONIA GOES "CLEAN"

North Macedonia has partnered with China in different areas over the past decade, most prominently on large infrastructure projects. The country joined the BRI partnership in 2014 and is also a member of the Cooperation between China and Central and Eastern European Countries (known as the "16+1" and later "17+1" Initiative). In 2018, cumulative Chinese funds put into North Macedonia through loan schemes and investments increased[15] more than 100 times compared to 2010, making China the second-largest economic partner of the country, ahead of the US and Russia. However, it was and still is trailing significantly behind the EU in this regard.

One of the most controversial Chinese deals is the yet-to-be-completed Kicevo - Ohrid highway, which went to have a staggering budget while being implemented in a procedure that did not comply with the public procurement legislation in North Macedonia. Moreover, the controversial selection of the main contractor 'Sinohydro' led to various wrongdoings that went under the spotlight in the wiretapping scandal in 2015[16]. Since then, some experts believe the Macedonian Government has been more cautious about entering into new partnerships with Chinese companies[17].

Despite the controversies that have marred the infrastructure partnerships between North Macedonia and Chinese companies, the Macedonian Government has been a steady partner of Chinese telecoms over the past decade. Huawei has been a significant player in the communications sector since 2010, when it opened its first branch. Besides partnering on Government-mandated projects, it has also established a foothold in the educational sector, donating computers to nearly 30 schools in Skopje, and helped to modernize the computer system in the Faculty of Computer Science and Engineering.

Huawei has also been keen on developing 5G infrastructure in the country before the strategic orientation of North Macedonia's Government took a turn in the other direction, away from its Asian ally.

In 2020, the Prime Minister in office at the time Zoran Zaev met Wang Yi, Chinese Minister of Foreign Affairs. They discussed future activities and strategies to broaden their partnership in various areas. Officials of North Macedonia and China have also discussed strategic electronic communications, including the construction of 5G networks. The US Embassy in Skopje took note of the meeting and warned against collaboration with Chinese companies that are "threats to national security and human rights."

A month later, North Macedonia would become the 11th country to sign the US Memorandum of Understanding "United States – Republic of North Macedonia Joint

Declaration on 5G Security"[18] and decided to limit the presence of "untrusted" communications companies in the country.

After the signing, Zoran Zaev said: "We have an obligation to align our telecommunications development policies with those of the EU as well as to align the security aspects of the implementation of the 5G network with our strategic ally, the US". Keith Krach, the US Under Secretary of State for Economic Growth, was not that subtle during his speech after the signing,[19] pointing to the need for "standing up against that doctrine of the Chinese Communist Party, threatening the privacy, security and data protection." After the NATO summit in 2021, where North Macedonia had its first presence as a full-fledged member, Zaev was asked if the Government would allow a Chinese company to build the 5G network in the country. He responded, "As a NATO member, that is unacceptable, on our soil and in any other member country." The course was set.

By signing the MoU, North Macedonia further aligned with the shared principles on 5G security outlined first in the 2019 Prague 5G Proposals[20] and in the EU's 5G Cybersecurity Toolbox, which is also called upon in the Clean Network. Neither China nor Huawei are mentioned in the Joint Declaration, but the references to 'Whether network hardware and software suppliers are subject, without independent judicial review, to control by a foreign government' appear to point to non-democratic and non-Western countries, such as China.

The EU published the aforementioned 5G Cybersecurity Toolbox in 2020[21] to identify some common measures that could reduce the most severe digital threats to 5G networks. China is not mentioned here either, and the toolbox includes all kinds of risks, not just government intrusion. Nevertheless, it states that governments can impose restrictions and exclude suppliers they consider a risk to critical functions.

The EU toolbox sets out a joint approach based on "an objective assessment of identified risks and proportionate mitigating measures" to address security risks related to the rollout of 5G. It also recommends excluding certain suppliers because their risk profile should generally be limited to the most critical and sensitive parts of the 5G networks.

5G IN NORTH MACEDONIA: (ROCKY) ROAD PAVED WITH GOOD INTENTIONS

Just months after North Macedonia joined the Clean Network Initiative, the Government proposed changes to the Law on Electronic Communications.[22] The amendments' purpose was "...to limit, prohibit and impose specific requirements and conditions based on risk assessment, regarding the supply, use, and operation of equipment for electronic communications networks, to provide clean and secure electronic communications networks." The amendments also cite "the elimination of risks to national security" as one of the driving reasons for the proposals.
Then, in April 2021, the Parliament of North Macedonia adopted[23] the Law on Electronic Communications amendments, imposing stricter rules against purchasing 5G equipment from "untrusted vendors." The amendments prescribe that a risk profile assessment of all relevant suppliers and manufacturers of critical network equipment should be carried out "periodically" by the National Center for Computer Incident Response.

The legal amendments proposed new measures which seek to limit or exclude the use of equipment by telecommunications network providers classified as "high-risk." The new proposals came shortly after the Agency for Electronic Communications (AEC) invited telecommunications operators to express their interest in participating in the planned 5G frequency allocation auction in June 2021.

Huawei failed to win the bid,[24] giving way for Ericsson to seize it, a company that has thrived from the backlash against its Chinese competitors in Europe.

Media sources in the country reported that Makedonski Telekom, the largest telecommunications provider in North Macedonia (with 35% of shares owned by the Government of North Macedonia), ranked Huawei as a top bidder in the tender procedure for purchasing 5G equipment. But the same media sources point out that the Government later recommended telecommunications companies not to do business with the Chinese giant.[25]

The amendments to the Law on Electronic Communications envisage the adoption of two bylaws. The first one is the Methodology for assessing the risk profile of suppliers and network equipment manufacturers, followed by the List of critical components and sensitive parts of electronic communications networks. The bylaws provide the AEC with the power to decide on the level of risk of a certain telecommunications equipment supplier.

According to the risk methodology,[26] four factors must be considered when con-

ducting the risk assessment.
They determine whether the suppliers and network equipment providers:

✓ are under the supervision of a foreign government without independent judicial control;
✓ have publicly available information about their founders and business partners and their governing and managing bodies;
✓ support innovations and respect the copyrights and related rights and intellectual property rights;
✓ are financed transparently, according to the best procurement practices, practices for investments, and the conclusion of contracts.

The primary justification for adopting the risk assessment was national security and the need to protect critical infrastructure from the influence of third-country governments. However, the criteria that the AEC provides based on which it will perform the risk assessment may limit or completely exclude the possibility for certain suppliers to participate in the telecommunications network market if the AEC assesses them as "high-risk suppliers."

Legal experts from the country pointed out[27] several potential shortcomings of the Law and its bylaws. They especially emphasized the possibility of their retroactive application, which could hinder suppliers of older generation networks and even smaller suppliers that have nothing to do with 5G related services.

According to law professor Borce Davitkovski, the illegality of the draft bylaws stems from the non-compliance of the Law on Electronic Communications with the European regulations. Therefore, the entire legislation that Macedonia has or intends to adopt is not according to the European directives and standards, and it should be harmonized as soon as possible."

International experts agree[29] that the Law on Electronic Communications amendments are of overly broad application: They are not limited to 5G networks but cover a long list of parts of all (including existing) telecommunications networks and, therefore, could have a retroactive effect. No transition period seems to be provided, and no process is offered for the supplier to remedy possible technical deficiencies.

Consequently, the North Macedonian proposals deviate from the principles of transparency, legal certainty, nondiscrimination, and proportionality, which are fundamental principles of the EU Treaty and part of the applicable legislation in telecommunications.

CONCLUSION

The Republic of North Macedonia is a country that pursues EU membership. Therefore, it is trying to harmonize its telecommunications legislation with that of the EU. Strategically, the Government took steps to further its determination to side with the Western allies by entering into partnerships with the US, such as joining the Clean Network Initiative.

However, the Government has stumbled in its efforts to align its legislation with its strategic priorities. The Law on Electronic Communications changes seem to be guided by political motives first and national security second. As much as the phrase "national security" is mentioned in the relevant legislation, its meaning is devoid of substance when it tramples well-established European principles on transparency and objectivity. Moreover, by shunning companies such as Huawei in a non-transparent and arbitrary manner, the country risks straining its relations with China. Decisions eerily similar to those taken by the Macedonian Government led Huawei to initiate arbitration proceedings against Sweden due to their exclusion from the rollout of 5G network products and services in that country[30].

The Law on Electronic Communications and its bylaws deviate from the general principles of EU law (transparency, legal certainty, nondiscrimination, and proportionality). The very documents that they are meant to follow, most prominently the EU Toolbox for 5G Security, recommend that the criteria for risk assessment should be objective, transparent and proportionate, and risk assessment should be technologically neutral and not based on undefined policy criteria. Those principles are missing.

The criteria set out in the risk methodology have an overly broad focus. They focus on the origin of suppliers and the availability of information about their founders, business associates, and governing bodies. They also list generalities such as "Whether they support copyright and protection of intellectual property rights" without explaining that formulation. All in all, key legislation seems to follow political and non-technical criteria.

This, on the one hand, appeases the country's ambitions to become a member of the EU but at the same time counters the principles that the Union has established for assessing the risk of 5G suppliers.

RECOMMENDATIONS

- The Methodology for assessing the risk profile of suppliers and manufacturers of network equipment should be updated according to the principles established in the 5G Toolbox and the Treaty of the EU, especially in the specific procedure for risk assessment. The Methodology should specify what "periodically" means, ensure a transparent approach to the risk assessment, and specify its frequency. The principles outlined in the EU 5G Toolbox should guide this process.

- Special attention should be devoted to ensuring that suppliers of older generation networks such as 4G will not be affected by the amendments to the Law on Electronic Communications and its bylaws.

- North Macedonia should strengthen its cyber security groundwork through unified security measures and a transparency system to make itself less susceptible to nefarious practices. For this purpose, the Law on the Security of Networks and Information Systems proposed in 2019 should be adopted as soon as possible

- The US and the EU should encourage North Macedonia to fully implement the EU 5G Toolbox.

- China needs to demonstrate that it can maintain transparent objectives and foster a stable and secure environment with its partner countries, built on shared interests and values, and prevent stigmatizing its presence in Macedonia. The partnership between both countries may stimulate economic cooperation and lead to a more competitive communications sector. Both countries should ensure a partnership fully compatible with the EU accession process.

REFERENCES

[1] Nadège Rolland, A Concise Guide to the Belt and Road Initiative, https://www.nbr.org/publication/a-guide-to-the-belt-and-road-initiative/

[2] Paul Triolo, Clarise Brown, Kevin Allison, and Kelsey Broderick, "The Digital Silk Road: Expanding China's Digital Footprint," Eurasia Group, April 29, 2020.

[3] Brigitte Dekker, Maaike Okano-Heijmans, Eric Siyi Zhang, Unpacking China's Digital Silk Road, Clingendael Report, 2020, https://www.clingendael.org/sites/default/files/2020-07/Report_Digital_Silk_Road_July_2020.pdf.

[4] Benn Steil and Benjamin Della Rocca, "Belt and Road Tracker," Council on Foreign Relations.

[5] "The Digital Side of the Belt and Road Initiative Is Growing," Economist, February 6, 2020.

[6] Robert Greene, Paul Triolo, Will China Control the Global Internet Via its Digital Silk Road, https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

[7] Stefan Vladisavljev (2021). China's 'Digital Silk Road' Enters the Western Balkans. Prague, Czech Republic, Association for International Affairs (AMO). Accessed on March 1, 2022.

[8] Pavlićević, Dragan. "A Power Shift Underway in Europe? China's Relationship with Central and Eastern Europe under the Belt and Road Initiative." In Mapping China's "One Belt One Road" Initiative, edited by Xing Li. Palgrave, 2018.

[9] Wendy Robinson (2020). The Trojan Dragon Comes to the Balkans. The Fletcher Forum of World Affairs Vol. 44, No. 2, A Return to Great Power Competition (SUMMER 2020), pp. 29-44.

[10] Chinese snooping tech spreads to nations vulnerable to abuse, Dusan Stojanovic, The Associated Press, October 17, 2019, https://apnews.com/article/9fd1c38594444d44acfe25ef5f7d6ba0

[11] Total Surveillance Law Proposed in Serbia, SHARE Foundation, September 2021, https://www.sharefoundation.info/en/total-surveillance-law-proposed-in-serbia/.

[12] "The Clean Network", The US Department of State, https://2017-2021.state.gov/the-clean-network/index.html. Accessed on March 15, 2022.

[13] U.S. House Of Representatives Intelligence Committee, "Investigative Report On The

U.S. National Security Issues Posed By Chinese Telecommunications Companies Huawei And ZTE," October 8, 2012.

[14] Trump Administration Issues Dual Orders Targeting Huawei and Economic Espionage, https://www.hugheshubbard.com/news/trump-administration-issues-dual-orders-targeting-huawei-and-economic-espionage

[15] Institute for Democracy Societas Civilis – Skopje, Chinese and EU 28 Cumulative Investments in North Macedonia (2010-2018), https://idscs.org.mk/en/2020/09/17/infographic-chinese-and-eu-28-cumulative-investments-in-north-macedonia-2010-2018/

[16] Ana Krstinovska, Exporting Corruption? The Case of a Chinese Highway Project in North Macedonia,https://chinaobservers.eu/exporting-corruption-the-case-of-a-chinese-highway-project-in-north-macedonia/

[17] Ivan Nikolvski and Zoran Nechev, "Fortifying 5G Networks in North Macedonia: The Need for Western Partners", China Observers in Central and Eastern Europe, January 12, 2021, https://chinaobservers.eu/fortifying-5g-networks-in-north-macedonia-the-need-for-westernpartners/.

[18] United States – Republic of North Macedonia Joint Declaration on 5G Security, US Department of State, October 2020, https://2017-2021.state.gov/united-states-republic-of-north-macedonia-joint-declaration-on-5g-security/index.html#:~:text=The%20United%20States%20and%20the%20Republic%20of%20North%20Macedonia%20each,secure%20and%20resilient%205G%20architecture.

[19] 360degrees, „Zaev on the Memorandum for 5G with the US: It's Vital for Our Economy and National Security", https://360stepeni.mk/zaev-za-memorandumot-za-5g-so-sadtoa-e-od-vitalno-znachene-za-nashata-ekonomija-i-natsionalna-bezbednost/

[20] Prague 5G Proposals, https://www.nukib.cz/en/infoservis-en/conferences/prague-5g-security-conference-2019/.

[21] Secure 5G Networks: the EU Toolbox, European Commission, January 2020, https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

[22] Law on Electronic Communications, Official Gazette of the Republic of Macedonia Nos. 9/2014, 188/2014, 44/2015, 193/2015, 11/2018, and 21/2018 and Official Gazette of the Republic of North Macedonia Nos. 98/2019, 153/2019, and 92/2021.

[23] Law on Electronic Communications, Official Gazette of the Republic of Macedonia Nos. 9/2014, 188/2014, 44/2015, 193/2015, 11/2018, and 21/2018 and Official Gazette of the

Republic of North Macedonia Nos. 98/2019, 153/2019, and 92/2021, https://www.mioa.gov.mk/sites/default/files/pbl_files/documents/legislation/zakon_za_izmenuvanje_i_dopolnuvanje_na_zakonot_za_elektronski_komunikacii-slvesnik92od2021.pdf

[24] Vladimir Mircheski, Macedonian Telekom Rolls Out 5G Network: Eriksson "in", Huawei "out", https://360stepeni.mk/makedonski-telekom-startuvashe-so-5g-mrezha-erikson-in-huavej-aut/

[25] Government asks "Makedonski Telekom" not to buy 5G equipment from Chinese "Huawei", 360 Stepeni, Vladimir Mircheski, September 15, 2020, https://360stepeni.mk/video-vladata-bara-od-makedonski-telekom-da-ne-kupuva-5g-oprema-od-kineski-huavej/.

[26] Methodology for Assesment of the Risk Profile of Suppliers and Manufacturers of Network Equipment, Agency of Electronic Communications, https://aek.mk/wp-content/uploads/2021/08/20210730_Metodologija-veb.pdf

[27] Ljupka Noveska Andonova, Veton Kjoku, Telecommunications Cleanup, Sloboden Pecat, https://www.slobodenpecat.mk/telekomunikaciska-generalka/

[28] Interview with Professor Borche Davitkovski, published on September 21, 2021, https://www.mkd.mk/makedonija/ekonomija/davitkovski-zakonot-za-elektronski-komunikacii-treba-itno-da-se-promeni-i-da-se

[29] Morgan Lewis, The approach of the EU and selected Member States to 5G Network Cybersecurity, https://www.morganlewis.com/pubs/2021/09/north-macedonia-proposals-should-follow-european-unions-balanced-risk-based-cybersecurity-approach#_ftn1.

[30] Huawei takes Sweden to court over 5G ban, https://www.thelocal.se/20220131/huawei-takes-sweden-to-court-over-5g-ban/, January 31, 2022