August 2020

Brief

# Between the Chinese Dragon and American Eagle

## 5G development in the Baltic states

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Maya Guzdar | Tomas Jermalavičius

**NATO cyber experts have called 5G the 'digital nervous system of the contemporary societies.'[1] But with the increased connectivity offered by 5G, however, comes an exponential rise in the number of potential targets for espionage. The Baltic states have begun to heed the warnings of their principal ally, the United States, who is calling to end cooperation with the Chinese telecom giant Huawei. The governments of the Baltic states are discovering that road to 5G development is becoming increasingly complex and fraught with geopolitical and national security considerations.**

## 5G and Geopolitics in the Baltic Region

The Baltic region has been dubbed a 'poster child' for early cases of 5G use due to the region's recent history of technological innovation. Its ambitious energy, communication and transport infrastructure projects as well as agriculture, forestry, advanced manufacturing, financial, IT, logistics and other industries and services are well situated to benefit from 5G adoption.[2]

Estonia has committed to achieving 5G connectivity in major cities and their periphery by 2023 and in transport corridors by 2025. It was under Estonian presidency that the EU released a year-by-year 5G roadmap for all member states.[3] Estonia's plans for a 5G frequency auction have been delayed multiple times due to the Covid-19 pandemic as well as legal action by Levikom, the fourth largest communications operator in Estonia, who sued the government for planning to auction off only three frequencies. The government has now opened up the auction to four frequencies but has endured criticism from Elisa Eesti, Tele2 Eesti, and Telia Eesti, the three largest operators in Estonia who claim the reduced frequency bands are too small to support a stable 5G network.[4]

Latvia is one of the first countries to push out a 5G network, and ranks third in Europe for 5G readiness.[5] Its largest operator Latvijas Mobilais Telefons (LMT) established the first working 5G base in Riga and, alongside Tele2 Latvija, has built 5G base stations that offer mobile users access to the 5G network. Bite Latvija, Latvia's third largest operator, is still testing. Latvia hosted their first 5G frequency auction in December of 2017, at which the 3.4-3.8GHz frequencies were auctioned off to LMT. Both Tele2 and Bite have since also acquired spectrum frequencies and in June of 2019, agreed to merge networks in Latvia and Lithuania.[6]

By 2025, Lithuania plans for its 5G network to cover all urban territories, international land transport corridors and other highways, main railway lines, airports and seaports. The implementation of its 5G connection is slated to begin in 2021, after the state's first spectrum auction that planned for the end of 2020, where operators Telia Lietuva, Tele2 Lietuva, Bite Lietuva, and the state-owned Telecentras are likely to bid.[7] Yet much of this plan is dependent on the resolution of spectrum interference conflict with Russia. Russia's 'digital territory' covers more than one-third of Lithuania due to the spectrum use by the Russian military radars and satellite communication stations in Kaliningrad exclave. This 'frequency occupation zone' has so far prevented Lithuania from

auctioning the 3.5GHz frequency, which is used throughout Europe for 5G.[8] The Lithuanian authorities, in cooperation with Poland and Latvia, are trying to alleviate the problem and also seek to engage Russia and Belarus in negotiations to resolve it.[9]

The extent to which Huawei is integrated into Europe's pre-existing 3G and 4G networks could cause years of slowdowns if Baltic governments were to ban the use of its equipment; according to Telia Lietuva chief technology officer, the U.S. is 'ten years too late' in its attempts to ban Huawei in Europe as countries have already invested tens of millions of euros into their 5G development.[10] Telia Lietuva is not alone in relying on Chinese technology in the Baltics, as Huawei currently provides equipment for Bite Latvija and Elisa Eesti, among others.

China's broader influence in the Baltic region cannot be ignored in the 5G context. China is one of the Baltic states' largest trade partners outside of the EU, and the region possesses key predispositions to become a Chinese equipped distribution centre in the Baltic Sea for cargo transportation as part of the Belt and Road Initiative. Baltic policymakers and business leaders often tout China as an important export market and source of investments. The Baltic states are also part of the 17+1, a cooperation framework created in 2012 between China and 16 Central and Eastern European countries to facilitate the arrival of Chinese investments and technology in the region.[11]

*Ensuring continuous presence of the U.S. forces in the region is one of the key objectives of the Baltic states' defence policies. The U.S. appears to have leveraged this in the discussions with the Baltic capitals about Huawei and 5G*

Chinese companies have also been active in shaping public perceptions in the Baltics: by the end of March 2020, Lithuania had received over 20,000 protective masks and 120,000 pairs of gloves from Huawei and other Chinese companies to help fight the Covid-19 pandemic—aid that Lithuanian security analysts believe was in part meant to soften the Lithuanian approach to Chinese involvement in 5G.[12] In November 2019, Huawei and Estonia's University of Tartu signed a memorandum of understanding to cooperate more actively in supporting studies, research and infrastructure development. Controversy ensued in February 2020 when an article on the risks and benefits of this partnership was rejected for publication in the university's journal.[13] The university's authorities denied Huawei's influence in the decision to block the article, yet asserted that the university 'should not get involved in political debate' of this sort.[14]

The Baltic states, however, remain staunch transatlanticists eager to continue strengthening political, security and economic relations with the United States. As the threats posed by Russia have only grown in recent years, the U.S. involvement in the region—including the support provided through the European Deterrence Initiative—has acquired ever greater importance to Baltic security. Ensuring continuous presence of the U.S. forces in the region is one of the key objectives of the Baltic states' defence policies. The U.S. appears to have leveraged this in the discussions with the Baltic capitals about Huawei and 5G: according to some media reports, in March 2019, in a meeting with Lithuanian prime minister Saulius Skvernelis, the U.S. ambassador cautioned that Huawei's equipment could 'create a vulnerability for allied troops' hosted by the Baltic states.[15]

Baltic cooperation with the U.S. also extends into cyber and energy security—sectors where introduction of 5G will be particularly important. Furthermore, the U.S. is a pivotal stakeholder in the Three Seas Initiative (3SI), a partnership of twelve countries between the Baltic, Adriatic, and Black seas aimed to promote investments in digital, energy, and transport infrastructure connecting them.[16] Many states involved—including the Baltics—view the partnership as a means for channelling the American investments to the region, thus providing the U.S. with another platform to advance its 5G and China stance, particularly given that much of the strategic infrastructure involved will certainly rely on services enabled by 5G technology. The upcoming 3SI summit in Tallinn, in autumn 2020, will show if Washington is inclined utilise this format to align 5G approaches across the region.

As a result of the shifting international security landscape, the 2019 reports by intelligence and counterintelligence agencies of Estonia, Latvia and Lithuania highlighted China's growing influence activities and espionage operations in each country and underscored that the use of Chinese technology by both the private and public sectors represented a significant security risk.[17] The increasingly close military relationship between China and Russia in recent years has also become a matter of concern that is certain to feature in 5G security assessments by the Baltic states.[18]

## Baltic 5G Stance

On 31 October 2019, U.S. vice president Mike Pence and Estonian prime minister Jüri Ratas signed a joint declaration on 5G network security to start a 'rigorous evaluation of providers.' The declaration, while never mentioning Huawei by name, effectively bans the company as it states suppliers 'should not be subject to control by a foreign government without independent judicial review.'[19] The declaration also requires transparent financing and structures, best practices, intellectual property rights, and a clean track record regarding respect for the rule of law, among others. It endorsed the Prague Proposals—a set of recommendations signed by over thirty countries that was created in May of 2019 for nations to consider as they construct and administer 5G infrastructure.[20] Estonian foreign minister Urmas Reinsalu, however, felt it necessary to underscore that the joint declaration addresses a national security issue and is not part of the U.S.-China trade war: 'I do not believe this could be treated as ruining our political relationship [with China] because the document makes no mention of specific companies.'[21] In response to the declaration, Estonian operators Telia and Tele2 have begun considering the use of Finnish Nokia or Swedish Ericsson for 5G technology.

On 12 May 2020, Estonia passed the 'Huawei law'—a set of amendments to the existing Electronics Communications Act which ensures security reviews by national authorities for new telecom gear. The law grants Estonia's Consumer Protection and Technical Regulatory Authority the right to impose an obligation on operators to provide information on the hardware and software used in the network. The government is also granted the authority to require operators to apply for authorisation for the use of communications network hardware and software.[22]

On 27 February 2020, Latvia and the U.S. signed a Joint Declaration on 5G Security. The declaration reaffirms the European Council's 'Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G' and the Prague Proposals. It stipulates that both countries will curtail the use of network hardware whose suppliers are subject to control by a foreign government, network hardware and supplies who do not have transparent structures of partnership, and suppliers who have a record of unethical behaviour. One of Latvia's largest mobile operators, Bite Latvija, having partnered with Huawei to launch a test 5G base station in June of 2019 and having worked with Huawei to develop a country-wide narrowband internet of things network for the past five years, is now uncertain of the prospects of its projects.[23]

After completing the European Commission's 5G security risk assessment, representatives of the Lithuanian government found no reasons to ban the use of Huawei equipment for civilian purposes.[24] Yet Lithuania's overall stance is likely to harden, as strategic considerations are becoming more salient. According to Lithuania's foreign minister Linas Linkevičius, following Estonia's and Latvia's examples, Lithuania plans to sign a memorandum on 5G with the U.S.[25] Defence minister Raimondas Karoblis called for common EU and NATO's position with regard to restrictions on the use of China's technology in 5G networks, but indicated that China's 5G technology might be anyway blocked from use in the Lithuanian national defence system.[26] Furthermore, Lithuania's legislative framework provides for screening and vetting of investors into enterprises of strategic importance to

*Whole-of-society awareness of potential threats and resilience to inevitable economic, diplomatic, cyber and informational coercion by Beijing will be of paramount importance in future development of 5G networks*

national security.[27] The government can invoke this legislation to keep Huawei away from projects such as 5G infrastructure for the port of Klaipėda, railways, airports, secure state communications networks, or energy and gas transmission system operators, but not from the networks of the mobile operators.[28]

## Future Challenges

The Baltic states have yet to develop a range of specific regulatory measures that would provide for effective screening of investments, technologies, supply chains and services determining security of their 5G networks. Estonia is currently leading the way with its draft regulation that will provide basis for assigning a security score to manufacturers and assessing whether their 5G equipment is acceptable for various security-sensitive uses.[29] Even though the Baltic states have considerable experience and expertise in managing cybersecurity challenges, much will depend on their further ability to enhance their technological competence and administrative capacity, as well as on the capabilities and diligence of their technical, security, intelligence, and political authorities and private sector in keeping abreast of threats posed by China. Whole-of-society awareness of potential vulnerabilities and resilience to inevitable economic, diplomatic, cyber and informational coercion by Beijing will be of paramount importance in future development of 5G networks. It also remains to be seen how Russia will leverage its military's hold on 3.5GHz frequency bands: to obstruct and complicate development of 5G in parts of the region or—with a long-term view of benefiting from its partnership with China and from Huawei's involvement as vehicle to increase the espionage opportunities in the Baltics—to exert pressure in China's behalf.

## Endnotes

[1] Kadri Kaska, Henrik Beckvard, and Tomáš Minárik, *Huawei, 5G and China as a Security Threat* (Tallinn: CCDCOE, 2019), 5.
[2] Will Townsend, "Latvia And Its 5G Path to Prosperity," *Forbes Magazine*, 6 December 2019.
[3] Urve Palo, "EU 2017 5G Roadmap," Ministry of Economic Affairs and Communications of Estonia, 2017.
[4] Kristjan Kallaste, "Period of Public Consultation in 5G Frequency Tender Extended," ERR, 17 June 2020.
[5] "Riga to Play Lead Role in European Agenda for 5G," *Amima Magazine*, 5 November 2019.
[6] Tom Leins, "A Guide to 5G Spectrum Auctions in Eastern Europe: the Baltic States," TeleGeography, 19 July 2018.
[7] "Lithuanian Government Endorses 5G Development Plan," Lrt.lt/BNS, 4 June 2020.
[8] Dan Jones, "Russia Reserves 3.5GHz Band for the Military, Not 5G," Light Reading, 20 August 2019.
[9] Tautvydas Lukaševičius, "Russian military a barrier to 5G development in Lithuania," Lrt.lt, 25 July 2019.
[10] Algirdas Igorius, "Lithuania Ready for 5G, but Only Chinese Companies 'Can Provide Full Package'," Lrt.lt, 31 July 2019.
[11] Andrew Chatzky and Lindsay Maizland, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, 12 February 2020.
[12] Linas Jegelevičius, "Chinese Facemasks: Don't Look a Gift Horse in the Mouth?," Baltic News Network, 22 April 2020.
[13] "University of Tartu and Huawei Signed a Memorandum of Understanding," University of Tartu, 27 November 2019.
[14] Aili Vahtla, "Paper: University of Tartu Refused to Publish Article on Huawei," ERR, 26 February 2020.
[15] "Reuters: US Ambassador Pressed Lithuanian Government on Huawei," Delfi.lt/BNS, 5 June 2019.
[16] "Three Seas Initiative (3SI)," Ministry of Foreign Affairs of Estonia, last updated 20 July 2020.
[17] State Security Department of the Republic of Lithuania and Second Investigation Department under the Ministry of National Defence, *National Threat Assessment 2019* (Vilnius: VSD & AOTD, 2020), 32-33; Estonian Foreign Intelligence Service, *International Security and Estonia 2019* (Tallinn: Välisluureamet, 2020), 59-62; Latvian State Security Service, *Annual Report on the activities of Latvian State Security Service in 2019* (Riga: Valsts drošības dienests, March 2020), 6.
[18] Vaidotas Beniušis, "China's cooperation with Russia and Belarus a 'risk factor' for Lithuania," Lrt.lt/BNS, 1 June 2020.
[19] "United States–Estonia Joint Declaration on 5G Security," The White House, 1 November 2019. According to China's 2017 National Security Law, Chinese companies are legally bound to 'support, provide assistance, and cooperate [with the government] in national intelligence work.' See Murray Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, 31 October 2019.
[20] Sten Hankewitz, "Estonia and the US Sign a Memo on 5G Security, Exclude Chinese Huawei," Estonian World, 8 November 2019.
[21] Marcus Turovski, "Foreign Minister: Estonia-US 5G Memorandum Will Not Hurt China Relations," ERR, 28 October 2019.
[22] Riigikogu (Parliament of Estonia), "Electronic Communications Act," *Riigi Teataja,* RT I 2004, 87, 593, translation published 28 May 2020.
[23] "Latvia Sides with US in Huawei 5G Fight," LSM.lv/LTV Panorāma, 20 February 2020.
[24] "Lithuanian PM meets with Chinese ambassador amid growing tensions over Huawei," *The Baltic Times/BNS,* 20 March 2019.
[25] "Lithuania Sets Guidelines for 5G Development," Lrt.lt/BNS, 28 May 2020.
[26] "Lithuanian defmin says decisions on Huawei technologies must be made at NATO, EU level," *The Baltic Times/BNS*, 4 June 2019.
[27] Seimas, "Republic of Lithuania Law on the Protection of Objects of Importance to Ensuring National Security," No XIII-992, as last amended on 12 January 2018.
[28] "Baltics Caught between Superpowers in China's 5G Battle – Investigation," Lrt.lt/Verslo Žinios, 10 September 2019.
[29] "Ministry drafts bill aimed at curbing Chinese 5G tech," ERR, 27 July 2020.

## About the Authors

Maya Guzdar is a research assistant at ICDS. She is a junior at Stanford University majoring in International Relations and minoring in human rights focused on East Asia as well as national security.

Tomas Jermalavičius is Head of Studies and Research Fellow at ICDS.



ICDS.Tallinn
@ICDS_Tallinn
ICDS-Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076