issue BRIEF
2019-05

Opportunities and Challenges for South Korea in the New Era of 5G

J. James Kim, Research Fellow
Hong Sanghwa, Research Associate
The Asan Institute for Policy Studies
2019.03.21

Introduction

2019 will be a watershed moment for global information technology (IT). It will mark the first time that the commercial 5G service will go operational nationwide in South Korea. Studies suggest that the 5G technology will offer data transmission speeds 10 to 100 times faster than the current 4G Long-Term Evolution (LTE) networks. This will not only allow faster exchange of data, it will open up new possibilities for the application of Artificial Intelligence (AI) in areas such as development of autonomous vehicles or drones and construction of smart cities, among others. This *Issue Brief* will explore the process by which South Korea has moved forward with the initial stages of this process and point out some of the challenges associated with the transition to a new nationwide IT infrastructure.

5G and the Fourth Industrial Revolution

5G wireless technology presents an enormous opportunity for South Korea but most of the critical breakthroughs will likely come from business-to-business (B2B) interactions in the near future. According to a survey of executives conducted by GSMA in 2017, for instance, the business community expects much of the new revenues to come from services in the B2B rather than the business-to-consumer (B2C) and business-to-government (B2G) domains (Table 1).[1]

South Korea's three major mobile carriers (KT Corporation, SK Telecom Co., Ltd., and LG U Plus Corp) are expected to invest a total of KRW 20-25 trillion (USD 20-25 billion) in laying down the 5G network infrastructure.[2] Of this amount, KRW 7.4812 trillion (USD 7.48 billion) will be allocated to building 5G base stations during 2019-23 (Figure 1).[3] Initial deployment will be focused around major cities including the Seoul metropolitan area.[4] Considering the time needed to commercialize the software products for 5G network, commercial 5G services are not likely to be in widespread use until 2023.[5]

[Table 1] New Sources of Revenues for 5G[6]

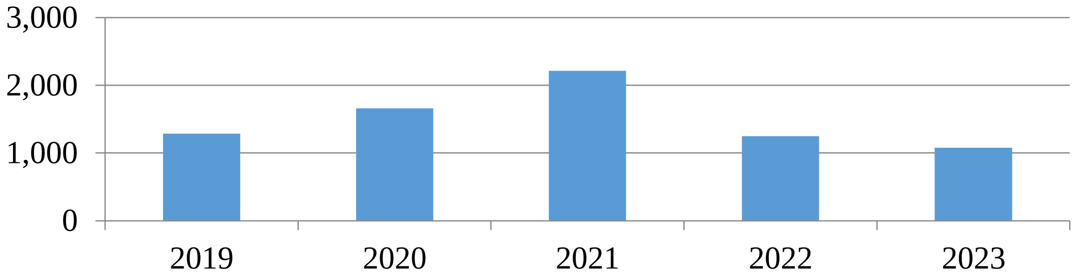
	Most important	Important	Moderate	Less important	Least important
Business (B2B, B2B2C)	**69%**	20%	3%	6%	3%
Consumer (B2C)	23%	31%	34%	9%	3%
Government (B2G, B2G2C)	14%	26%	40%	17%	3%

Source: GSMA(CEO 5G Survey, October 2016)

According to a report released by the KT Economic and Management Research Institute,[7] South Korea's 5G network is expected to inject at least KRW 30.3 trillion (USD 30.3 billion)[8] into the South Korean economy by 2025, which will be 1.51 percent of the country's gross domestic product (GDP) in 2025. The report estimates that this number would grow to at least KRW 47.8 trillion (USD 47.8 billion) by 2030 (2.08 percent of the GDP). Companies are striving to develop new 5G services that can yield such growth.

Figure 1. Investment in 5G Base Station (KT, SKT, LG U plus)

(Unit: USD million)

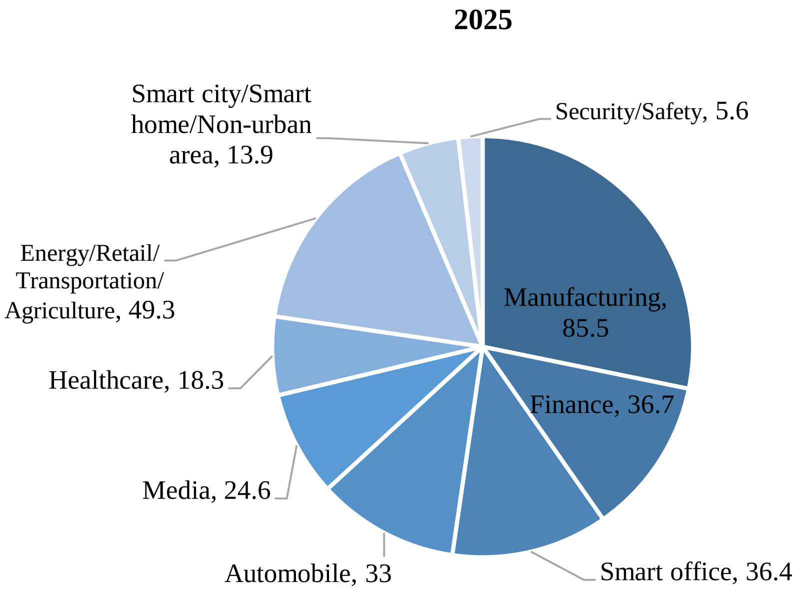


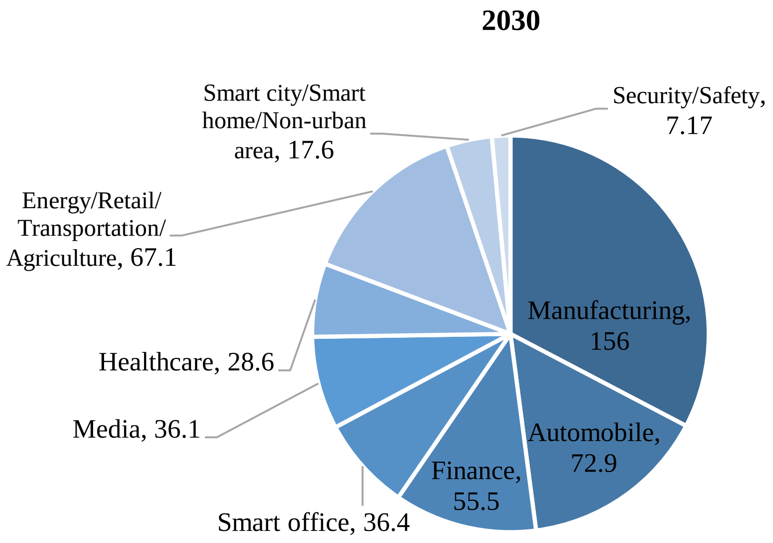
Source: National Assemblyman Song Hui-gyeong[9]

The Moon administration sees the 5G wireless technology as the launchpad for South Korea's takeoff into the Fourth Industrial Revolution.[10] The impact is expected to be significant on all sectors of the economy. In manufacturing, for instance, the next-generation smart factories would enable companies to reduce supply chain costs and improve quality. Usage of autonomous driving and truck platooning is expected to become more pervasive. More widespread use of big data, AI, and biometric authentication would also bring about a paradigm shift in the financial sector. 5G would open the floodgates for higher quality virtual reality and augmented reality, which will change immersive media experiences. Significant transformation is also expected in the healthcare industry as people will have easier access to their own health data. Remote surgery and medical treatment may become easier and more widespread. Drone usage in courier service is expected to shorten delivery time and cost. Retail industry will focus even more on inventory and logistics rather than physical displays and showrooms. In agriculture, development and application of smart farming are expected to increase agricultural productivity.[11]

Figure 2. Value-Added by 5G

(Unit: USD 100 million)





Source: KT Economic and Management Research Institute

Much of the research and development among the country's three major mobile carriers are focused on realizing these socio-economic benefits (Figure 2). To support this effort, South Korea's Ministry of Science and ICT announced a plan in October 2018 to invest KRW 86.3 billion (USD 86.3 million) by 2020 in five areas: smart factory, smart city, autonomous vehicle, immersive media, and disaster/safety.[12] In December 2018, the National Assembly passed a special tax law to reduce the tax burden among the three major South Korean mobile carriers by allowing a tax deduction equivalent to 3 percent of the investment in 5G base stations established outside of Seoul, Incheon, and Gyeonggi Province during 2019-20.[13]

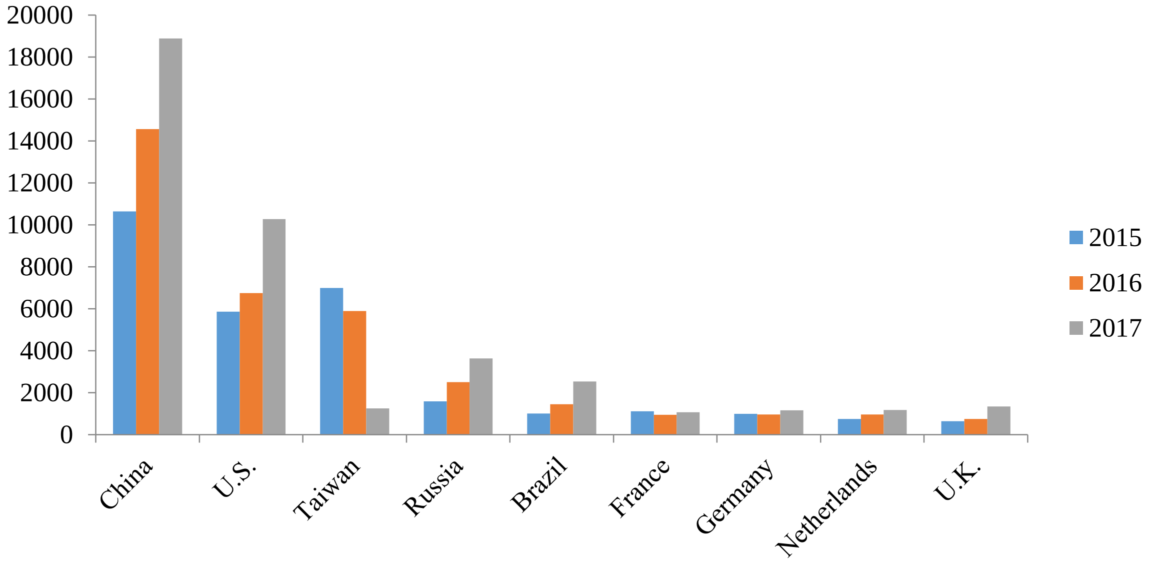
Security Challenges

While there are clear benefits to the nationwide deployment of 5G services, South Korea must also address some serious concerns related to its dependence on Chinese equipment and technology. In particular, LG U Plus relies on Huawei equipment and technology for some of its 5G network. As of December 2018, 5,804 5G base stations have been installed nationwide by the three major mobile carriers. Among them, 4,133 stations are operated by LG U Plus in Seoul and Daejeon metropolitan area.[14] While it is not clear how many of these stations are linked to Huawei, there is growing pressure on LG U Plus to exercise greater caution and transparency in its utilization of Chinese equipment and technology.

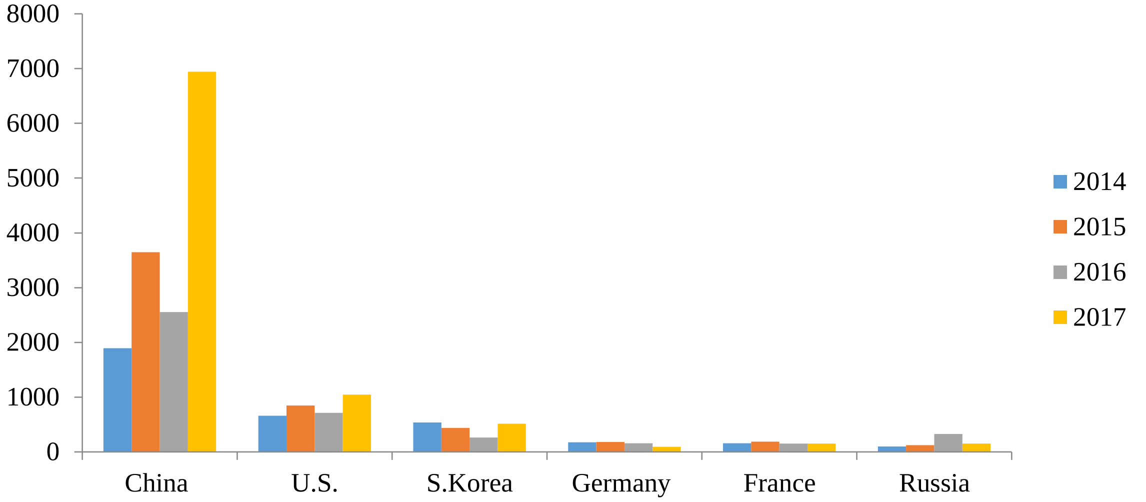
Research has shown, for instance, that a significant number of cyberattacks against government agencies and companies around the world have originated from China.[15] In a recent report by the cybersecurity company Carbon Black, China and Russia accounted for nearly half of all politically motivated cybersecurity incidents between July and November of 2018.[16] Some of these incidents are linked to the Chinese government and companies like Huawei and ZTE. Huawei, for instance, is facing a 10-count indictment by the U.S. government for violating T-Mobile's intellectual property rights and evading U.S. sanctions against Iran through its subsidiary Skycom Tech Co Ltd.[17] The Chinese government, in coordination with Chinese telecommunications companies, have also been found to have transferred confidential data from the headquarters of the African Union to servers in Shanghai over a period of five years without prior consent.[18] Bloomberg's recent report about tiny spy chips in Supermicro server motherboards widely used by many U.S. companies also raised concerns about the potential for Chinese hardware hack.[19] This report was especially disconcerting due to the fact that Chinese companies supply approximately 75 percent of all mobile equipment and 90 percent of all computer parts around the world.[20]

These incidents, while not isolated, have raised concerns among many countries about the national security implications of relying on Chinese technology. According to an unpublished memo released by the U.S. National Security Council on January 30, 2018, China has invested quite heavily in 5G network development.[21] The report goes on to recommend that the U.S. must temper its dependence on China's 5G technology. This view is widely shared among other countries such as Australia, Canada, New Zealand, Japan, France, Germany, and the Czech Republic.

Figure 3. Incidence of Cyberattacks Against the South Korean Government, 2015-17[22]



Incidence of Cyberattacks Against the South Korea's Ministry of Foreign Affairs, 2014-17[23]



South Korea must begin to take this threat seriously given that its government agencies continue to be the target of cyberattacks from mainland China (Figure 3). Both hardware and source code hackings pose a serious threat to South Korea's national security. South Korean authorities are currently investigating how many Supermicro motherboards are being used in the country and are considering remedial measures to address this security weakness.[24] However, the government response related to the usage of Chinese equipment in 5G networks has been relatively subdued. The official position is that the South Korean government will refrain from intervening directly in the day-to-day operations of private telecommunication companies.[25] Instead, the government has encouraged LG U Plus to respond to these security concerns through third-party inspection of Huawei source codes. The results of this finding is likely to be made public during the first half of 2019.

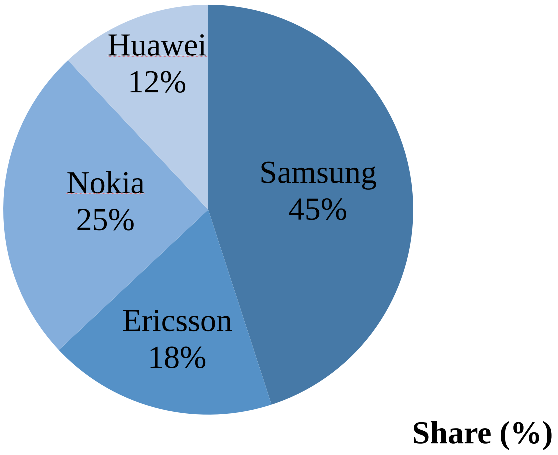
Meanwhile, LG U Plus has argued that the management and operation of the telecommunications system is different in South Korea from other countries like Australia and the United States. In the former, the network system is managed by service providers whereas in the latter, equipment providers manage and operate the networks themselves. LG U Plus also argues that the company's 5G network is not connected to the external network and that it is thoroughly monitored and managed by its staff. Critics argue that these conditions do not preclude every possible ways in which security can be breached in the LG U Plus operated network.[26]

Table 2. Geographic Distribution of 4G LTE Network in South Korea

	Samsung	Ericsson	Nokia	Huawei
SKT	Capital area, Chungcheong	Gyeongsang	Jeolla, Gangwon	-
KT	Capital area, Busan, Ulsan	Gangwon, Chungcheong (north), Gyeongsang	Chungcheong (south), Jeolla	-
LGU+	Chungcheong, Jeolla	Chungcheong, Jeolla, Gangwon	Gyeongsang, Capital area (south)	Seoul, Capital area (north), Gangwon

Source: Eugene Investment & Securities[27]

Figure 4. Distribution of 4G LTE Equipment in South Korea



Source: Eugene Investment & Securities[28]

5G is also only a part of the story. South Korea must seriously reconsider its dependence on Chinese technology and equipment in 4G LTE. This is because the transition to 5G will be phased in over time with 4G LTE expected to play an important role in this transition. This is especially so given the fact that the 5G network will initially operate in a Non-Standalone (NSA) mode. That is, the 5G services will utilize existing LTE networks in the initial onset of its deployment. This is an intermediate temporary arrangement which is expected to be phased out in the long run as the 5G infrastructure becomes more robust and established. This is also partly why the mobile carriers that provided the 4G LTE services are also the preferred providers of the 5G network. Based on available data, Huawei gears account for a small but significant portion of the total 4G wireless network (Table 2, Figure 4).

Conclusion

The 5G network holds many promises for South Korea's economy and society. However, there are significant risks associated with the government's decision to permit the use of Chinese equipment and technology. South Korea has attempted to manage this risk through diversification of equipment and service providers. However, this does little to address the vulnerabilities in the network and which can be exploited by outside actors. More stringent regulation and oversight are critical to safeguard South Korea's national security.

These efforts must also move beyond a narrow focus on 5G. Naver, South Korea's biggest web portal, is reportedly using Huawei equipment and technology in its new Internet Data Center (IDC). Given that the company offers cloud services for various government agencies and public entities, this decision has raised some eyebrows in South Korea. Naver executives claim that Huawei devices and equipment are not used in the Pyongchon IDC, which handles all cloud services for government and public institutions.[29] This, however, does not address the potential security breach in the private domain.

Reliance on Chinese technology and equipment in wired network is even more disconcerting. KT Corporation, for instance, has recently announced its decision to use Huawei equipment for NongHyup Bank's network upgrade project, one of the country's four major commercial banks. Huawei's transmission equipment will be used to build the major network lines connecting 6,200 NongHyup Bank branches across South Korea. As the network provider for all major financial institutions, KT may also choose to utilize Huawei equipment for the three other largest financial institutions (i.e. Shinhan Bank, KB Kookmin Bank, and KEB Hana Bank).[30]

Due to Huawei technology's strong price competitiveness, dependence on Huawei equipment extends beyond South Korea's financial institutions to other key areas of the economy. For instance, Huawei has been chosen to supply the backbone networks for both the Korea Securities Computing Corporation[31] (Koscom) and the Korea Electric Power Corporation (KEPCO).[32] Huawei also provides the core equipment for telecommunications systems in Seoul Metro lines Nos. 1 to 4 and Nos. 7 and 8.[33] These arrangements together with past pattern and practice suggest that South Korea is vulnerable to potential cyber-attacks in strategic sectors of the economy.

It is important that the South Korean government takes these threats seriously and attempt to find a robust solution to address the vulnerabilities in its IT infrastructure. One possibility is to phase out the South Korea's reliance on Chinese equipment and technology. This is justifiable in the sense that there are adequate alternatives to Huawei, such as Samsung, Nokia, and Ericsson. The other is to continually invest in the development of better cybersecurity system. It is important to recognize that there is no single one-size fits all solution to this problem – that is, cybersecurity requires continual adaptation and development. Finally, instead of leaving cybersecurity to individual firms, it may be best to pool the expertise and resources of both the public and private sector. Developing a more cooperative and open arrangement between the government and businesses may be an ideal approach to addressing this shortcoming.

[1] The government urged mobile carriers to make 5G consumer service available at affordable price. IBK Economic Research Institute, *5 Sedae Idongtongsin(5G)i Gajyeool Mirae: Jungso Tongsinjangbigieobege Hojaeinga* (June, 2018); LG Economic Research Institute, *5G Service Ga Neomeoya Hal Gwajedeul* (February 9, 2018).

[2] IBK Economic Research Institute, *Op. Cit.*; LG Economic Research Institute, *Op. Cit.*

[3] National Assemblyman Song Huigyeong, *Tongsin3sa 5G Tuja Yeoryeokbujok, Yesangaek Mot Michineun 7 Jo 5000 Eokwon* (October 11, 2018).

[4] As of November 30, 5,804 5G base stations were set up across the country by the three mobile carriers. Among them, 3,858 (66.5%) stations were established in the Seoul Metropolitan area, whereas only 173 (2.9%) stations were set up in Busan. National Assembly Yun Sangjik, *Idongtongsinsabyeol 5G Gijiguk Singo Hyeonhwang* (December 7, 2018).

[5] IBK Economic Research Institute, *Op. Cit.*

[6] Question: Where will new operator revenues in 5G come from? (https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download)

[7] KT Economic and Management Research Institute, *5G Ui Sahoegyeongjejeok Pageubhyogwa Bunseok* (August 1, 2018).

[8] We assume an exchange rate of USD 1 = KRW 1,000.

[9] National Assembly Song Huigyeong, *Op. Cit.*

[10] Remarks by President Moon Jae-in at Fifth Stop of Nationwide Economic Tour: Daejeon as Special Fourth Industrial Revolution City, January 24, 2019 (https://english1.president.go.kr/BriefingSpeeches/Speeches/113)

[11] KT Economic and Management Research Institute, *Op. Cit.*

[12] Ministry of Science and ICT (MSICT) Press Release, *Mingwani Sonjabgo 5G Meokgeori Balgul Naseonda* (October 4, 2018).

[13] If a company's employment rate grows by more than 5 percent year-to-year, there is an additional one percent deduction in addition to the two percent baseline deduction.

[14] National Assembly Yun Sangjik, *Op. Cit.*; Lee Sangjae, "Guknae Yuseonmang Kkwak Jabeun Huawei, 2inja ChepoBulttong Tuina," *JoongAng Ilbo*, December 9, 2018.

[15] Center for Strategic & International Studies, *Significant Cyber Incidents* (https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity)

[16] Carbon Black, “Destructive Cyberattacks Increase Ahead of 2018 Midterm Elections,” *Quarterly Incident Response Threat Report*, November 2018.

[17] United States of America v. Huawei Device Co., LTD. And Huawei Device USA, Inc., United States District Court for the Western District of Washington at Seattle. Indictment (No. CR19-010), January 16, 2019.

[18] Joan Tilouine and Ghalia Kadiri, “A Addis-Abeba, le siège de l’Union africaine espionné par Pékin,” *Le Monde*, January 26, 2018.

[19] Jordan Robertson and Michael Riley, “The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies,” *Bloomberg Businessweek*, October 4, 2018.

[20] Gwon Bongseok, “Bloomberg Choecho Bodo ‘Supermicro Hacking chip’ Sageon Jinsileun,” *ZDNet Korea*, December 23, 2018.

[21] NSC, “Secure 5G – Flipping the Script,” *Unpublished Memo*, January, 2018. (https://docs.house.gov/meetings/IF/IF16/20180130/106810/HHRG-115-IF16-20180130-SD1011-U1011.pdf)

[22] National Assemblyman So Byeonghun, *Jinanhae Jeongbubucheo·◌Gwangyeokdanche Hacking Sido 7Man 5,724Geon* (October 13, 2018).

[23] National Assemblyman Park Juseon*, Park Juseon Uiwon, “Oegyobu Hackingsido Choegeun 5Nyeongan 4Man2Cheonyeogeon”* (October 1, 2018).

[24] The National Intelligence Service (NIS) manages cybersecurity for government and public organizations while the Ministry of Science and ICT (MSICT) handles companies in the private sector. Im Mincheol, ‘Jeongbu “Portal·Tongsinsa Supermicro Server Hyeonhwang Josajung”,’ *ZDNet Korea*, October 16, 2018.

[25] Kim Dongpyo, ‘Jeongbu “Huawei 5G Boan Munje, Itongsa Seuseuro Gyeoljeonghaeya”,’ *Asia Business Daily*, October 4, 2018.

[26] Park Sungwu, “中 Huawei Tongsinjangbi Doib Chujin LG U plus, Boan Issue e ‘Jinttam’,” *Chosun Biz*, October 31, 2013; Seong Hocheol, ‘LG U plus “Oebu Internet Manggwa Bunridwae 中 Huawei e Tongsinjeongbo Yuchul Wheomseong Eobseo”,’ *Chosun Biz*, November 1, 2013.

[27] Park Jongsun and Han Byeonghwa, “5G Sangyonghwa Service Sunhang Jung!,” *Eugene Mid-Small Cap Issue Report*, September 18, 2018.

[28] Park Jongsun and Han Byeonghwa, *Op. Cit.*

[29] Lee Gyeongtak, “Jeongboyuchul uryeoedo Huawei Jangbi Sucheondae Gumaehan Naver,” *Digital Times*, April 24, 2018. G-Cloud is a government cloud computing platform for central administrative agencies. Public officials in local governments maintain their own cloud system. Private-sector cloud services must comply with strict security requirements established by the Korea Internet & Security Agency (KISA) and the National Intelligence Service (NIS) to have access to government and public organizations. The Special Committee on the Fourth Industrial Revolution under the National Assembly, *Gukhoe 4 Cha Saneobhyeokmyeong Teukbyeolwwonhoe Hwaldonggyeolgwabogoseo* (May 2018).

[30] Kwon Gyeongwon, “‘5G Jangbi·◌Yuseonmang Eotteokehana’…Huwawei risk e Gosimhaneun Hankuk,” *Seoul Economic Daily*, December 10, 2018.

[31] Koscom is the financial IT solution company owned by the Korea Exchange (KRX).

[32] Lee Sangjae, *Op. Cit.*

[33] Baek Jiyeong, “‘Gagyeok Huryeochigi’ 中 Huawei Gongpo…Gukga Gigan Infrakkaji Doksik Uryeo,” *Digital Daily*, May 23, 2018.