



5G and the Future Internet

**Implications for Developing Democracies
and Human Rights**

Rumana Ahmed, Elizabeth Sutterlin, Moira Whelan
National Democratic Institute

July 2021

5G and the Future Internet

Implications for Developing Democracies and Human Rights

Rumana Ahmed, Strategic Planning, Technology, and National Security Consultant

Moira Whelan, National Democratic Institute

Elizabeth Sutterlin, National Democratic Institute

Table of Contents

Executive Summary	3
Understanding and Prioritizing Strong 5G Networks	5
What is 5G Technology?	5
Who Controls 5G Systems Within a Country?	6
Why a Secure 5G Network?	6
Global Development Impacts for Developing Democracies.....	8
Social, Economic and Environmental Implications	8
Regional Trends for 5G Adoption.....	9
Implications for Democracy and Human Rights.....	9
Global Influencers in 5G and Future Internet Technology	12
Global Standardization Bodies	12
Other Digital International Organizations and Initiatives	12
Countries Influencing Global Digital Landscapes	13
The Oversight Role of Parliaments, Civil Society and Other Stakeholders	15
Recommendations for Further Research	17
Acknowledgments	17
References	18

Executive Summary

Communication infrastructures are the cornerstone of our societal interactions. The rapid development of new generations of information and communication technology (ICT) increases our dependency and vulnerability on less hardware that is increasingly powerful. The fifth generation of the communications network (5G) revolution is already here, and discussions for 6G are underway. 5G will transform the way we communicate and live. It will expand information access and control, bring billions of devices online across sectors, automate everyday activities, and advance smart cities and policing. These developments, however, bring risks to public interests, and have national security and human rights implications.

5G adoption is happening throughout the world. At the end of 2019, almost 200 countries had announced plans to invest in 5G,¹ and by the end of 2020, 52 countries launched commercial 5G services.² While the COVID-19 pandemic has delayed the deployment of 5G infrastructures globally, it has also cast a spotlight on the need for reliable digital technologies for remote work, education, healthcare, and service delivery. While the focus and demand for 5G is rooted in economic ambition, the impact on the rights of citizens must also be considered.

Events over the last ten years have demonstrated that technology is inseparable from the future of democracy. Automated disinformation fueled public division in Latin American elections. Artificial intelligence (AI) surveillance allowed the Chinese government, under the control of the Chinese Communist Party (CCP), to target protestors in Hong Kong. Internet shutdowns obscured free elections in Guinea and Uganda and censored democracy protests in Myanmar. Technology is increasingly used to block transparency and suppress dissent in closed and closing spaces, violate privacy and individual rights, and polarize societies even in the most vibrant democracies. Technologies reliant on 5G infrastructures could further enable these negative impacts on democracy and civic participation, due to the volume, scope, and scale of data that will be accessible through 5G.

Democracy stakeholders have yet to craft 5G strategies that protect privacy, human rights, and democracy. The lack of familiarity with the technology limits the ability to identify effective interventions. Questions on how democracy is impacted by 5G starts with how they are built, who provides and controls it, and how it is regulated. The architecture and use of 5G networks must be underpinned by security, corporate responsibility, democratic norms and principles. The democracy community has a key role to play in engaging the public, companies, governments, and global entities on 5G. This White Paper is a *first step* towards a few objectives:

- Understanding paths to 5G in developing democracies to inform democracy donor countries, as well as national and local democratic actors to include governments, parliaments and CSOs;
- Understanding the players involved in the rollout of 5G infrastructure and how they interact with democratic actors;
- Identifying implications 5G could have on democratic activity; and
- Outlining gaps and research needed for next steps in identifying and strategizing on possible points of intervention and action by the democracy community.

To develop this white paper, NDI conducted initial research and interviews and developed a database of 5G adoption in countries in which it works. To further develop an understanding of how countries approach technology issues, NDI inventoried countries in which government shutdown or cybersecurity laws had been adopted. Upon completing the research, NDI consulted with six think tanks and private-sector experts on approaches, opportunities, and risks to 5G expansion. From this research, some key findings include:

Democracy Context for 5G

- 5G expansion is an active and ongoing discussion by government actors in all countries NDI works in, including countries with low Internet penetration. 5G is a question of when, not if. Multi-stakeholder engagement on decision making around 5G or other technology issues was not readily evident. In most country cases, parliaments and legislatures are weak in general, and even more so on technology related issues.
- Decision-making around 5G adoption occurs almost exclusively in executive branches of government with little to no oversight of these actions.
- Research conducted on 5G expansion is focused almost exclusively on its impacts on security and economic growth. Although some literature alludes to potential risks to human rights, no comprehensive research exists in the NGO/academic community. There has also been no research on the impacts—positive or negative—on democracy.
- 5G adoption in a country inclined toward authoritarianism makes autocrats more effective and efficient in achieving that end by expanding illiberal capabilities to undermine democratic norms and human rights.
- Almost 64* of the 98 countries researched are actively engaging corporations with close ties to the CCP on 5G. 42 are engaging companies without such ties.

Challenges and Threats

- The influence of the CCP over the digital landscapes and 5G standards gives autocratic leaders broader control over data flow and local governance.
- Mass surveillance augmented by 5G could empower large-scale human rights abuses like mass discrimination and persecution.
- With 5G-backed AI capabilities, deep fakes will have higher resolution, look more real, and more people have access to make them. Leaders will have real-time access to citizens' information and attention to employ subversive information tactics to foster polarization, cynicism, and political disengagement.
- Global civil society organizations are actively involved in monitoring technology adoption to include 5G, but almost no dedicated organizations focus on these issues within the context of their country. Inclusion of civil society around 5G issues appears to not exist.
- Although research exists on the potential impacts of technology on women and marginalized communities, no in-depth research was identified linking the potential impact of 5G on these communities and their engagement in democratic processes.

Approaches on Intervention and Future Research

- Even if leaders come to different conclusions about the risks and acceptable trade-offs of 5G within their country, prioritizing policies and systems that uphold democracy is critical.
- Democracy communities have yet to effectively exert strategic influence in the global digital arena. Democratic actors must work together across sectors to advance technology that upholds democratic norms and human rights.

Understanding and Prioritizing Strong 5G Networks

What is 5G Technology?

New generations of technology come along almost every ten years. The fifth generation, or 5G, is an advanced mobile technology that is expected to be one hundred times faster and have a thousand times more capacity than previous generation technologies. 5G will transform the Internet as we know it. It can deliver fast and reliable connectivity, wider data flow, and machine-to-machine communication. 2G gave users access to voice calls and basic text, 3G drove video and social media services, and 4G made digital streaming and data-heavy applications possible. 5G is anticipated to be a dramatic leap forward for artificial intelligence (AI) and entire smart cities.³ It will enable the Internet of Things (IoT), in which everything from electrical grids to hospital systems to running shoes will be interconnected online.⁴ Remote robotic surgery will be routine, and autonomous vehicles will travel along smart highways. 5G is expected to drive global growth and its economic effects realized by 2035.

Companies Leading Global 5G Network Development

Huawei, ZTE, Nokia, Ericsson, and Samsung are leading the charge to expand 5G. These carriers typically interface with local telecom companies, and some provide end-to-end equipment and maintenance services.

5G Carrier	HUAWEI	NOKIA	ERICSSON	ZTE	SAMSUNG
5G Equipment Market Share	30%	15%	14%	11%	2%
5G Commercial Contracts	91+	139	124	55	9
Global Presence (in countries)	170	130	180	140	80
Standard Essential Patents	1554	1427	819	1208	1316

Source (2021): <https://foreignpolicy.com/2020/01/22/5g-cellular-huawei-china-networks-technology-infrastructure-power-map/>

Huawei (China): Huawei is the largest telecom RAN equipment company and the second largest core network infrastructure producer. Huawei's rise since 2010 has been driven by a 695 percent increase in their R&D budget and Chinese government subsidies that have allowed them to make its products the most affordable in the market. As of 2020, they shipped over 600,000 5G base stations (cell towers designed for localized coverage).

Ericsson (Sweden): Ericsson led the equipment market, before being surpassed by Huawei in 2016. Since 2010, Ericsson's R&D spending increased 23 percent and are the largest core network infrastructure producer. Ericsson was among the first in the ICT to incorporate rights and digital inclusion in their corporate guidelines.

Nokia (Finland): Nokia, along with Ericsson, dominated market shares in the era of 3G and 4G. However, both have both relied on China for sensitive equipment within their supply chains.

ZTE (China): ZTE is China's second-largest telecommunications equipment manufacturer. ZTE is particularly competitive in the global mobile device market.

Samsung (South Korea): Samsung is the only company besides Huawei to provide total end-to-end 5G solutions, including chip sets, base stations, and smartphones. Samsung has shipped over 100,000 base stations, but is still far behind in the network market.

Figure 1: Countries Leading Global 5G Network Development

Who Controls 5G Systems Within a Country?

The primary components of 5G include the spectrum, core network, radio access network (RAN), and end-user device. A spectrum is like fuel for the 5G ecosystem. It is the range of all types of electromagnetic radiation and frequencies. The radio spectrum is the part of the spectrum used for telecommunications, broadcast, and more. When it comes to infrastructure and data transmission, the core network acts as a hub for data. The RAN provides coverage through small local cell towers at base stations that transmit data to and from devices. Within a 5G network, the RAN has more control than the core in processing data, making it a focus within a cybersecurity framework. Today, Huawei is the leading RAN equipment distributor, followed by Nokia. Carriers connect devices and transfer data through the core network and RAN, while providers sell the service to clients and users. Components of the ICT system are each controlled by public and private sector entities.

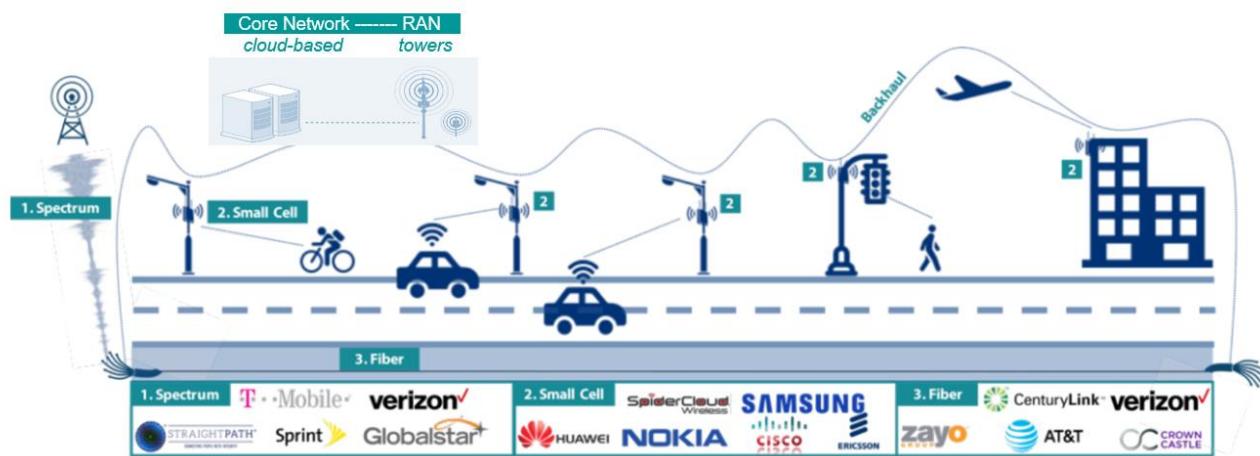


Figure 2: Core Components of a 5G Network

Government agencies control the spectrum and designate which companies and entities can use which frequencies, and sign contracts with international or local carriers and providers to establish 5G networks. In some countries, 5G is managed by independent carriers and providers. In other instances, some carriers, local providers, and service platforms are owned, partially-owned, or heavily influenced by emperors and governments. In Thailand, China, the Middle East, and Africa, these carriers solidify the rule of governments and subvert the rights-based order.⁵

Why a Secure 5G Network?

The strength of 5G is that the core and periphery of a network are one. Like a new car with a faulty engine, the decentralized and interdependent nature of ICT systems means that any one insecure component of an ICT system can have a rippling effect on the safety, economic well-being, and rights of its users. 5G networks will enable flows of personal data, transmit content that informs and shapes perceptions, and supply critical infrastructure. The immense economic opportunities that 5G presents should not be passed up; instead, it is imperative that the democracy community prioritizes security, transparency, privacy, integrity, and quality of these networks. Insecure governance structures, including equipment governance, around 5G systems will be vulnerable to risks that affect institutions, businesses, and people.

Vulnerabilities and Impacts of an Insecure 5G Network

Bribery by influencers like the CCP, with a stated prioritization of AI and tech supremacy, offer debt relief and investments. Such predatory economic behavior inhibits innovation and violates OSCE guidelines and corporate anti-corruption measures.	Equipment quality and data integrity issues of hardware or firmware could impact service reliability, such as for surgeons working from miles away, critical infrastructures during a natural disaster and users' privacy.
Privacy, data loss, and data misuse by carriers or providers using network maintenance access capabilities to intercept and share data with their home or local governments for illiberal use. "Maintenance" makes covert hacking no longer necessary.	Long-term risk mitigation costs for governments and companies can be significant. While companies like Huawei offer reduced acquisition costs (free equipment), maintenance costs (software bugs, data loss, coding) can be greater.
Network surveillance, censorship and shutdown demands by illiberal host governments compel cooperation by providers, carriers, applications or platforms. They can influence to whom data flows.	Broaden the digital divide and close open spaces for women, rural areas, and civil society. Current uneven distribution in the access to 5G, illiberal uses of ICT for rights abuses could be compounded by 5G.
Security and critical network attacks can expose those who rely on them. The risk of cyberattacks on 5G-dependent installations (power, water) could have repercussions for communities' human rights. ⁶	No oversight by governments and providers. Lack of transparency over data controls leave 5G risks misunderstood. Lack of public awareness creates an accountability vacuum.

Figure 3: Vulnerabilities and Impacts of an Insecure 5G Network

A strong and secure 5G system conducive to democracies is made of trustworthy equipment, follows a legal framework, and is managed by companies and governments that prioritize human rights and democratic norms to preserve free and open societies. It includes global standards and policies that protect values, promote inclusion and ensure accountability. Figure 4 below maps the components and stakeholders in a secure 5G ecosystem.

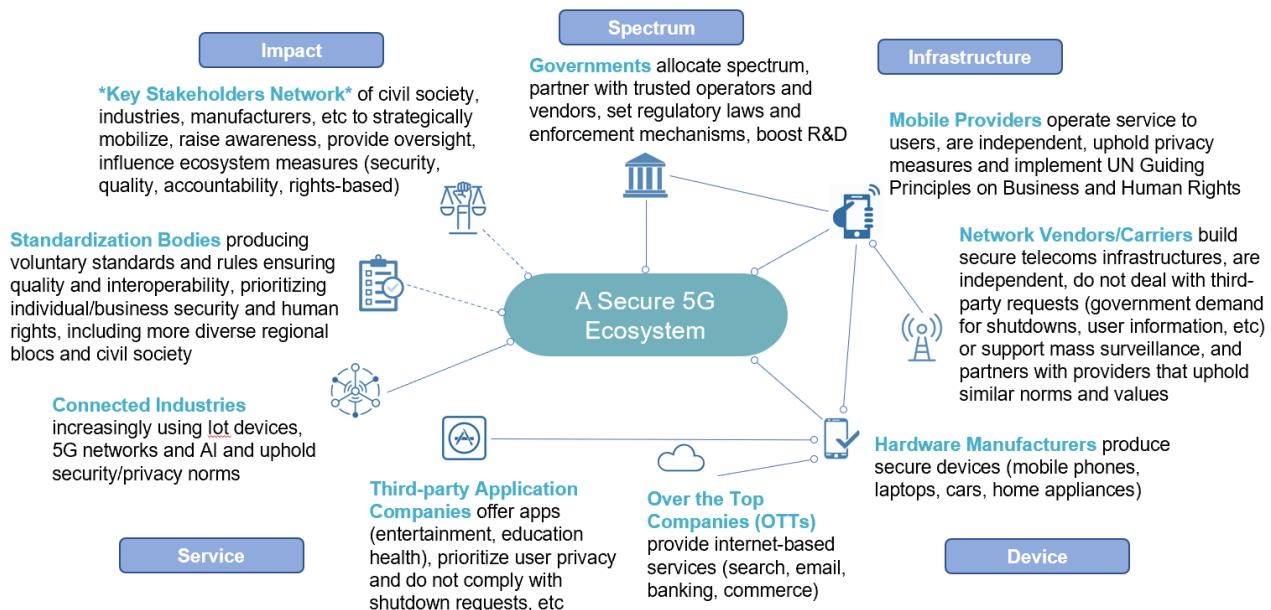


Figure 4: A Secure 5G Ecosystem

Choosing 5G network partners is a decision of risk. For developing democracies who have taken historical steps to progress rights, growth, and security, the decision needs to be rights-based. 5G infrastructure

investments now will set the groundwork for future technologies, so it is essential that this infrastructure preserves free and open Internet and societies.

Global Development Impacts for Developing Democracies

Social, Economic and Environmental Implications

The demand for 5G is growing. NDI's analysis shows that even countries with low internet penetration are engaging in 5G discussions. Advocates of 5G within the United Nations (UN), see it as a vehicle to bridge the digital divide between developed and developing, men and women, and rural and urban. 5G is expected to catalyze social and economic growth in what some refer to as the "Fourth Industrial Revolution." Some experts interviewed for this project worry that without extensive government and company investments, 5G could widen the divide. Even as countries come to different decisions on the economic benefits, risks, and acceptable trade-offs of 5G, prioritizing technological infrastructures, standards and partners that uphold democracy, individual security, and human rights will be critical.

	Projected Opportunities of 5G	Projected Challenges of 5G
Economic Growth	5G is expected to increase GDP and lead to greater productivity. In developing countries, it will improve infrastructure, transportation, delivery services, and smart city initiatives.	Insecure 5G networks could be easily compromised, having harmful economic externalities due to increased network reliance, and lead to long-term economic costs and affect stability and development.
Environmental Impact	5G with IoT will increase energy efficiency, reduce greenhouse gas emissions, reduce water and food waste, and enable more use of renewable energy. Connected devices (sensors, smartphones) will share data, enabling smart cities to be more sustainable through automated regulation.	Ericsson projects 5G will have 5.8 billion mobile subscriptions and 125 billion IoT devices by 2030. 5G could be responsible for one-fifth of all electricity consumption and generate 14% of greenhouse gas emissions globally by then. Without an energy efficient system, 5G will not be sustainable.
Rural Access	5G offers the potential to increase access to more people, especially in rural areas. The global pandemic has renewed focus enabling remote work, healthcare, and education for rural communities. ⁷	Without government incentives, rural areas remain costly to develop 5G. The UN expects 68% of populations to live in cities by 2050, which may make smart cities a priority over rural communities. ⁸
Social and Gender Equality	The UN's ITU is mainstreaming digital access and gender equality through advocacy, public-private partnerships, and global standards. ⁹ 5G is also anticipated to increase connectivity and close the digital divide among persons with disabilities (PWDs.)	Despite growing Internet and mobile uptake, the gender digital divide is growing globally, and women will likely bear the brunt of 5G-enabled abuse through deep fakes and other forms of online harassment. Unequal distribution of 5G and lack of proactive measures, digital skills, and affordability will continue to be barriers to PWDs. ¹⁰
Individual Security and Rights	Consistent with the UN SDGs, equal access of all people to 5G systems should be a priority, and within a rights-respecting framework. Access offers more individual freedom to information and economic opportunity. It also offers governments increased capacity to deliver on services such as financial flows and emergency services. 5G offers more security and user data protection than its predecessors.	As technology evolves, so do its risks. Weak networks are susceptible to information manipulation and digital rights abuses via surveillance and censorship.

Figure 5: Projected Opportunities and Challenges of 5G

Regional Trends for 5G Adoption

Over half of the world's population is connected to the Internet. The U.S., Europe, and Asia Pacific are shifting from 4G to 5G. However, much of the Global South is still primarily on 2G and 3G networks—almost 90 percent in Sub Saharan Africa, 70 percent in the Middle East and North Africa, and 52 percent in both Latin America and Southeast Asia. Even within 5G advanced countries, disparities exist primarily between rural and urban connectivity.¹¹ While 5G promises to fast-track digital development, much of the world has yet to experience 4G.¹² Still, countries in every region are exploring 5G. Of the 170 countries Huawei operates in, at least 69 have signed 5G contracts without restrictions. Huawei's longstanding telecoms presence defines their reach.¹³ Without intervention, data indicates that around 64 of NDI's partner countries are unlikely to ban Huawei for these reasons.

Who countries partner with 5G and how they use it could have a regional diffusion effect. Europe is seeking to prioritize security-based partnerships. Southeast Asia has been on a democratic decline since 2018, as governments imprison opposition leaders, persecute minority groups, and adopt statist methods for Internet control.¹⁴

Implications for Democracy and Human Rights

In our analysis, NDI has established that there has been little focus on the democratic and human rights impacts of 5G in geopolitical and security debates, market decisions, or public coverage. Yet the effects of disruptive technological change have proven to be significant in democracies. 4G has already ushered in a new phase, in which technology is both a tool for civic mobilization and the dissemination of information as well as a tool for misinformation, surveillance, censorship, and exploitation by antidemocratic forces. Any 5G-backed technology promises to increase the scope and scale of its democratizing power to influence information spaces, civic participation, and human rights. However, illiberal actors are using the same tools to drown out and suppress these spaces and rights within emerging democracies.

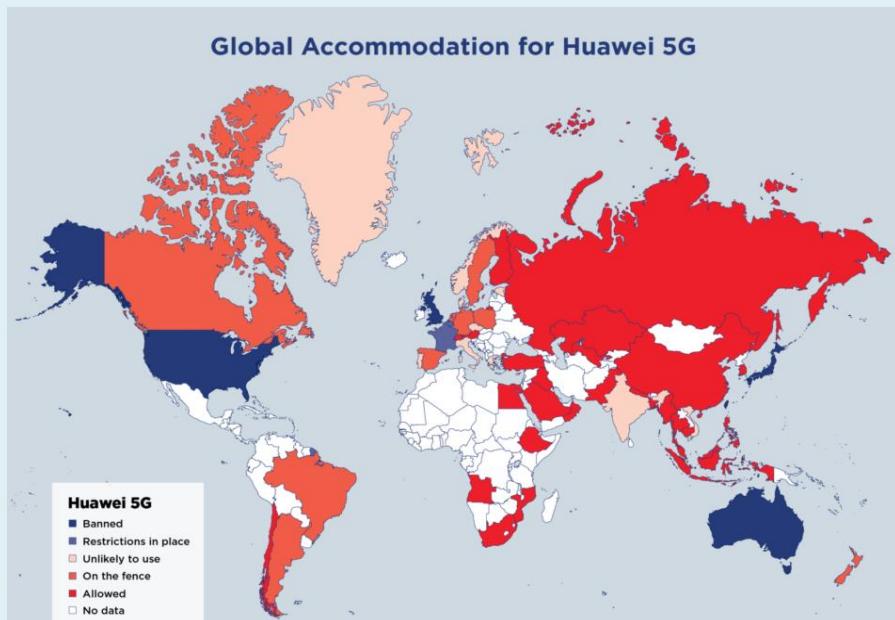
Mobilization and Innovation

5G technology can expand the scope of technological innovation and accelerate data flows that could improve elements of successful democracies. 5G opens new opportunities on livelihoods and increased data capacity that can make democracies more efficient and enable governments to deliver on services. Utilities will be linked using 5G making them more energy efficient and emergency services could broaden reach as well as have more increased and reliable connectivity which is critical for reaching rural areas. Perhaps the greatest promise of 5G as an indirect benefit to democracy is increased access for more people. Because connectivity is more efficient, more individuals will be able to utilize technologies sometimes not available in hard to reach spaces. For instance, live video which often fails or “buffers” in low connectivity places will improve. This increases opportunity for increased information flow, access to education tools and other societal benefits. Put simply, democracies have every reason to pursue and benefit from the technological promise of 5G. Recognizing the risks of any technology is always important. With 5G, the risks can be long term, expensive and do irreparable harm if not managed appropriately.

Country Case: Tunisia



Tunisia is the only state in the Arab world undergoing a form of democratic transition since the Arab Spring. Ten years and multiple governments later, the struggle for democracy continues as evident with the recent “Façade democracy” protests in January 2021. Tunisia is expanding its telecoms infrastructures, having among the highest connectivity in North Africa. The country's Telecommunications Act in 2013 officially abolished government internet censorship. They attempted to spotlight human rights by hosting RightsCon, a tech and human rights summit, the first time it was held in Africa or the Middle East.



Source (2020): <https://www.cnas.org/publications/reports/digital-entanglement>

Europe: In light of the U.S. ban on Huawei, more European countries (the UK, Poland, Romania, Estonia) are opting for alternative carrier companies or implementing restrictions. Nokia and Ericsson have moved to the forefront of 5G in the region. Still, Huawei maintains a strong foothold in the European Union (EU), owning 60 percent of its telecom contracts.

Southeast Asia: Huawei led the rollout of 4G networks across the region, making them the likely partner to upgrade to 5G. Myanmar and Cambodia already signed 5G MoUs with Huawei.

Africa: In 2019, the African Union signed a three-year MoU with Huawei to improve technical expertise, including 5G and smart cities projects. Huawei has built about 70 percent of Africa's 4G networks. South Africa was the first to sign a 5G commercial contract in the region.

Latin America: China has been investing aggressively in the region, spending \$110 billion between 2005 and 2018. Huawei has long partnered with many state-owned telecom companies. Chile, Brazil, Peru, and Colombia have signed MoUs with Huawei. Mexico has signed a commercial contract with Huawei to build out their core infrastructure for 5G networks. Venezuela has announced Huawei and ZTE investments to explore 5G.

Middle East: Gulf countries are leading the charge on 5G, signing massive contracts with Huawei. Among them are Saudi Arabia and Qatar state-owned companies, who also operate networks in Asia and Africa. Gulf countries also have contracts with Nokia and Ericsson.

Figure 6: Global Accommodation for Huawei 5G

Human Rights and Democratic Processes

The same capabilities of 5G that can bolster democracy can also be used to strengthen autocracy, undermine democratic norms, and commit widespread human rights abuses. *5G adoption in a country inclined toward authoritarianism makes autocrats more effective and efficient in achieving that end by expanding the scope and scale of illiberal capabilities.* In recent years, the world has witnessed the use of digital repression to undermine democracy around the world. Digital authoritarianism comprises techniques that are not mutually exclusive: cyber-attacks, social manipulation, censorship, Internet shutdowns and surveillance.¹⁵ Digital repression has dangerous chilling effects on participation, and can exacerbate social and political polarization, which threaten democratic processes and values, and the rights of citizens to have a voice in their governments.

Government-controlled 5G infrastructures could be detrimental to election integrity, free speech, and democratic participation. Given the widespread use of digitally repressive tactics by governments today, spurred on by tools and technologies from illiberal influences, these efforts are likely to accelerate under 5G infrastructure. From 2014 to 2016, Internet shutdowns were used in a third of the elections in sub-Saharan Africa,¹⁶ and in Uganda's contested 2021 elections, the incumbent president ordered state-owned Internet providers to block Internet connectivity. Huawei partners with Uganda, not only on 5G technology, but to surveil and track political opponents by intercepting encrypted messages and using mobile data as well.¹⁷ Israeli company Circles works with other autocratic governments to use cyberespionage tools to spy on human rights defenders, and journalists. Investigative reports indicate that Nigeria and Guatemala have used similar tools to spy on civil society actors.¹⁸ In these and other cases, illiberal actors are more than willing to exploit flaws in global mobile telecommunications infrastructure to locate citizens without warrants and intimidate those who speak out in closed and closing spaces into silence. *The Chinese government has also reserved the right to collect data on any device or application held by a Chinese company.* This makes Huawei and ZTE powerless against privacy violations by their government.¹⁹ Who they choose to share that data with and how they use it has yet to be seen.

As more connected devices (polling stations, voting machines and cards) rely on 5G, cyber attackers can expose network vulnerabilities to undermine democratic processes. Russian state-backed hackers leaked campaign emails targeting Hillary Clinton in the 2016 U.S. elections and Emmanuel Macron in France's 2017 elections, impacting voter confidence in the liberal candidates. Such interference can fuel mistrust and political disengagement. As some states pursue ambitious plans to move to online, remote voting and referendums, security for free and fair elections must be a priority, particularly in cases where illiberal states with high technological capacity could compromise the integrity of e-voting technology.²⁰

Mass surveillance tools, augmented by AI and 5G, could empower large-scale human rights abuses and mass discrimination. Surveillance already threatens the ability of marginalized people to participate safely in open civic discussions. 5G expands the capacity for data collection and the speed with which that data can be used. The CCP's surveillance state and use of facial recognition technology in Xinjiang to persecute its Uighur Muslim minority has become a prototype for large-scale "automated racism."²¹ At least 75 countries employ AI surveillance technologies under the pretext of smart city platforms and smart policing initiatives.²²

Country Case: Venezuela



President Nicolas Maduro welcomed ZTE's partnership on 5G and has taken Chinese investments to help offset Venezuela's humanitarian crisis. ZTE is exporting surveillance tools to help build a smart identification card system, similar to the one in China, to monitor social, economic, and political behaviors of citizens. Venezuela's smart cards are starting to track voting, and to link to subsidized food and health programs most citizens rely on to survive.

Social and Democratic Unity

With more personalized data and connected devices, micro-targeting and dissemination of misinformation at scale will undermine people's trust in institutions, in the media ecosystem, and in each other. The Philippines floods the information ecosystem with disinformation to harass critics, and the chilling effects this has on freedom of speech will only grow as 5G infrastructure makes state-sponsored trolling and harassment even cheaper. In 2017, officials and citizens used Facebook to spread disinformation to fuel hate and incite a genocide against Rohingya Muslims in Myanmar. During the 2018 elections in Brazil, Mexico, and Colombia, the three largest democracies in Latin America, politicians used artificial amplification to provoke fear and influence voters. False narratives, hyper partisan blogs, and "deep fake" altered videos fueled social and political polarization.²³ With 5G-backed AI capabilities, deep fakes will be more realistic and easier to produce. Leaders will have real-time access to citizens' information and attention to employ subversive information tactics that foster polarization, cynicism, and political disengagement. The CCP is already building information applications to simultaneously perform mass data collection and output propaganda to influence information environments at home. The export of such applications into the hands of illiberal influencers would be alarming.²⁴

Global Influencers in 5G and Future Internet Technology

While motivations and methods for 5G and Future Internet technologies differ, countries have been primarily focused on security. Democracy or human rights considerations remain mostly absent, allowing illiberal digital influencers to export playbooks for repression and supply equipment for misuse. Democratic stakeholders have fallen behind, but can still play a greater role in 5G and Future Internet standards, influence, and oversight. *"As Russia, China, and other states advance influence through forms of digital authoritarianism, stronger responses are needed from the U.S., democracy partners, and civil society to limit the effects of their efforts."*²⁵

Global Standardization Bodies

The International Telecommunication Union (ITU) and the 3rd Generation Partnership Project (3GPP) are the two main regulatory bodies that have jurisdiction to allocate spectrum frequencies, develop global technical standards, and facilitate global transfers of data across networks. They bring together global standard-setting organizations, companies, and regional telecommunications groups to develop protocols that can ultimately encourage diverse competition and security. The ITU, a UN agency, has promoted the shared use of 5G and future networks to address the digital divide. However, there are growing concerns that China is leveraging its extensive influence at the ITU to promote its own AI and Future Internet agenda, by muddying the waters on human rights underpinnings in the forums.²⁶ While standards adoption is voluntary, the ITU is among the few relevant multilateral forums for shaping the Internet and digital technology agenda. Their outputs are detailed, prescriptive and highly influential on states.²⁷ With so many members and key decisions being made, the ITU is among the few worth investing time and strategic effort for democracy and civil society stakeholders. Regional blocs from the Americas, Africa, and EU at the table have significant space to grow. Influencing regional and global policies and standards to prioritize rights will require engaging governments, other global initiatives and carriers, not just standard bodies, to build alliances.

Other Digital International Organizations and Initiatives

The EU and WTO are also particularly influential on technology agenda issues. Given the UN's interconnected role in 5G with the ITU, the UN is increasingly playing an influential role in Future Internet standards, making forums like the annual UN General Assembly an opportunity to engage members, build regional influence, and get rights-based technology issues on the global agenda for action. Some service

and technology provider companies, like Ericsson, are part of the Global Network Initiative (GNI), a multi-stakeholder initiative giving a more united voice on privacy rights issues within the ICT industry. Few civil society organizations are engaging on 5G technology issues at a global level, with far less representation from organisations based in the Global South. Rights-based organizations have been unable to strategically address technology rights issues across the various number of relevant policy forums. Some of the challenges they face include some forums being narrow in focus and highly technical, and having closed processes and memberships that limit civil society from having a voice in 5G discussions.²⁸ Increasing civil society and Global South voices in these forums is a clear gap with potential to create positive change.

Countries Influencing Global Digital Landscapes

China has promoted its vision of “cyber-sovereignty” to justify censorship and other digitally repressive practices at odds with democratic values of an open Internet, and now seeks to use international standards bodies to further solidify its model of Internet control. From 2017 to 2019, companies with ties to the CCP made every submission for surveillance standards to the ITU, and have already begun submitting 6G standard proposals. The U.S. and others have been far behind. At the ITU, the Chinese government advocated to remove mentions of “freedom of expression” and “multistakeholder” from underlying frameworks to exclude civil society and business voices. The Chinese government's influence over standards gives state-backed companies the advantage to build applications on top of 5G networks that use their equipment, allowing for broader access to data flow.²⁹ The CCP's model of digital authoritarianism is increasingly attractive for other autocrats seeking to use novel technologies to clamp down on dissent and consolidate power. In Zimbabwe, as part of a \$71 million Belt and Road Initiative investment, the government partnered with a facial recognition company with ties to the CCP to create a surveillance network similar to the one in Xinjiang.³⁰ Where exported, the CCP's model of data governance could further empower autocracies and threaten civil society, journalists, and activists who work towards inclusive and responsive democracies.

Russia is partnering with Huawei on 5G, but also employs more traditional methods of surveillance through intimidation and interference. Russia has deployed surveillance tools in both the near and far abroad, from countries like Belarus, Azerbaijan, and Ukraine to Nepal, Algeria, and Mexico. Russian surveillance relies on an ad hoc model that utilizes legal, technical, and administrative means to control information and intimidate civil society as well as Internet and telecom providers. This model is more well-suited for authoritarian regimes who have limited economic and technological resources, and may prove to be more adaptable than the CCP's high-tech model as they seek to expand their influence domestically and abroad.³¹

The Gulf states were among the first in the world to launch commercial 5G services, and have been investing heavily into 5G and advanced technologies. Local Arab service providers are partnering with ZTE and Nokia to expand their reach in Arab and Asian countries. In many Gulf countries, 5G and Internet service providers are predominantly government-owned, thus consolidating government influence over 5G-backed services or platforms.³² This could make requests for sharing data or Internet shutdowns easier for governments. Dubai is already deploying facial recognition technology developed by companies with ties to the CCP for its “Police without Policemen” program.

Israel and India are important influencers in global digital forums. However, the nature of their digital practices in the context of democratic backsliding raises concern. While Israel has awarded 5G contracts to local companies, it continues to export surveillance tools. According to a UN report, Israel's NSO spyware, usually sold to governments, is thought to have been used by Saudi Arabia to monitor journalist Jamal Khashoggi before his murder in Turkey.³³ Israel's military has used facial recognition in the West Bank to engage in mass surveillance to monitor Israelis and Palestinians on social media.³⁴ India's border security already uses Israeli-developed surveillance tools in Kashmir,³⁵ much to the concern of activists, and India regularly restricts internet access in Kashmir for long periods of time.³⁶ These trends in the use of

technology to surveil and repress people raise concerns over India's and Israel's willingness to support and practice democratic, rights-based global standards on 5G.

The United States issued a ban on Huawei from U.S. supply chains in 2019 over security concerns and pressed other countries to do so as well. However, many countries have long relied on telecommunications equipment from companies with ties to the CCP and are unlikely to ban Huawei. Japan, Australia, New Zealand, Sweden, Poland, the UK, and Czechia are among the few that adopted the ban. The Trump administration also launched the “Clean Network,” a proposed approach to protecting citizens’ privacy and companies’ information from the Chinese government and the CCP. But their narrow approach to targeting only vendors ignores the broader systemic threats and impacts underpinning 5G (i.e. digital inequality, social and political polarization, human rights abuses, censorship, automated discrimination). At the ITU, the U.S. has lagged in contributing towards setting critical 5G standards. Instead, in 2020, the U.S. Agency for International Development signed a deal with India and Israel to help implement 5G in developing countries, placing the U.S. in a questionable venue as it relates to 5G security and illiberal uses.³⁷ President Biden’s new administration can be a key player in making the U.S. approach comprehensive and in prioritizing the protection of democracy and human rights. A \$100 billion in broadband spending proposal by the Biden government is an important step that brings opportunity for affordability and could encourage other countries to do the same.³⁸

European countries are striving to emerge as leaders in setting global standards and developing secure 5G infrastructures. The EU is setting an example for implementing comprehensive oversight and regulatory policies. Sweden and its fellow Nordic countries signed a declaration aiming to be the first interconnected 5G region in the world. Sweden’s Ericsson is trying to expand in their foreign partnerships on 5G trials.³⁹ The Czech Republic hosted the first Prague 5G Security Conference in 2019, announcing a series of recommendations pertinent to the intersection of technology, economy, and privacy issues. The Prague Proposals frame cybersecurity as more than just a technical issue that requires national strategies, sound policies, a comprehensive legal framework and a network of dedicated experts.⁴⁰ France, the UK, and other countries that have restricted Huawei within their borders, have not done so for their carriers who can still use providers with ties to the CCP in developing countries where they operate. The issue of their security restrictions at home not affecting their firms’ operations and what equipment suppliers they use abroad is a concern for developing democracies. The democracy community can play a role in engaging these countries on the vulnerabilities for security and human rights that their firms may be complicit to beyond their own borders.

South Korea established itself as an early market leader for 5G development. Their networks within Asia will be instrumental in the diffusion of 5G development within the region. Currently, South Korean’s Samsung is primarily present in the 5G devices market. Samsung is under consideration as a replacement for Huawei in discussions by the “D10 Club,” a telecoms supplier group that was established by the UK and consisting of G7 members plus India, Australia, and South Korea. However, details of the D10 Club agenda have yet to be established. While South Korea and others attempt to expand their role in 5G, ICT decoupling from Huawei and security-trade tradeoffs are proving to make the process complicated.⁴¹

The Oversight Role of Parliaments, Civil Society and Other Stakeholders

The democracy community has yet to work effectively together to reach the maximum potential for strategic influence in the global digital arena or to advance rights-based approaches to technology and global standards for 5G, 6G, and the Future Internet. Global ICT forums lack regional representation of the Global South and civil society. Most global parliaments and legislatures do not have strong capabilities to conduct oversight or regulation on technology issues. Individual countries have yet to develop national strategies and alliances to secure comprehensive ICT ecosystems of diverse vendors, global standards, and investments in R&D.⁴² Creating and executing such efforts must involve governments, private industry, think tanks, and civil society to protect democracy and bridge the digital divide. Figure 7 lays out the responsible stakeholders for a 5G ecosystem below. The private sector alone can no longer drive these conversations.

Stakeholders Responsible in a Secure Rights-based 5G Ecosystem ⁴³				
<i>International Associations</i>	<i>Public-Private Partner Organizations</i>	<i>Regulators & Policymakers</i>	<i>Service/Technology Providers</i>	<i>Civil Society & Democracy Partners</i>
Enterprises, international associations, regional alliances	World Bank, IMF, OECD, UN, UNFCCC, 5G Infrastructure Public Private Partnership	Parliaments, government regulators, agencies and ministries	Network operators, manufacturers, equipment and service providers, platform companies	Democracy donors, civil society, think tanks, journalists, grassroots advocates

Figure 7: Stakeholders Responsible in a Secure Rights-Based 5G Ecosystem

The G7 issued a statement placing 5G security on the global agenda, but the UN can be a key venue to further prioritize rights-based systems. R&D investments in emerging technologies like software-based 5G solutions could be more cost-efficient, reliable, sustainable, and secure. Such investments would also make the equipment-centric approach dominated by companies with ties to illiberal actors like the CCP obsolete, paving the way for more secure and better rights-based software solutions. Ericsson is an example for corporations to conduct business from a rights perspective and to incorporate digital inclusion. Figure 8 lays out potential entry points for engagement for each of these actors.

Events over the past year have demonstrated that civil society and the public can play a role in shaping the applications and uses of corporate technology. In 2020, global protests over police brutality and advocacy efforts by the Algorithmic Justice League pressured Amazon, Microsoft and IBM to halt police use or development of facial recognition tools.⁴⁴ In Serbia and Uganda, journalists and NGOs conducted investigations to galvanize public pressure against their governments' usage of mass surveillance tools provided by companies with ties to the CCP. As more countries move towards 5G adoption in the near future, it is crucial that parliaments, civil society, and the public are engaged to ensure oversight of secure technologies that uphold democratic norms and human rights.

Potential Entry Points for Engagement	
Public & NGO Networks	<ul style="list-style-type: none"> • Understand the issues and risks and translate them to regional/country contexts; Learn the technical language and business, legal and economic angles • Develop a clear rights-based digital agenda, comprehensive proposed policies and actions; Identify and build key alliances and influential networks • Educate the public and impacted communities; Use media to generate interest, galvanize public pressure and expose tech exploitation by governments and companies; Advocate for expanding investments in digital skill
Local Parliaments & Governments	<ul style="list-style-type: none"> • Translate and educate the risks and steps to be taken from a human rights, democracy, economic, security, and political standpoint • Advocate for R&D investments in Future Internet innovation, diverse technological solutions and vendors; Update technology policies and regulations protecting privacy, human rights, and an open internet; Create policies, grants and business incentives for 5G investments and affordability in rural and marginalized communities • Work with relevant agencies to align 5G objectives and democratic values in development assistance partnerships, telecommunications bids, and spectrum allocation
Private Sector Industry	<ul style="list-style-type: none"> • Understand the players, relationships, and roles of different companies in the ICT system to develop proposals of policies to protect against government requests to platforms and local providers • Educate businesses on security risks, mitigation costs, and privacy/rights tradeoffs • Engage companies on standards to prioritize rights and security; to uphold their obligations and responsibility; to incorporate rights and digital inclusion into business model; to bring civil society voices and interests with them into global forums; to set metrics that evaluate partnerships for product risk, government risk, intended use; have transparent ownership, partnerships, corporate governance structures, and data collection and sharing practices • Establish public accountability measures and strategies for companies
Foreign Governments & Public-Private Organizations	<ul style="list-style-type: none"> • Engage governments that implement security restrictions on ICT at home, but that have companies operating in the Global South without the same security restrictions • Make rights-based approaches to technology and its use a global agenda issue through the UN to prioritize connectivity regulations and standards, establish a recommended 5G adoption digital roadmap for countries to follow • Engage open government partnerships and public-private organizations on tying rights to funding mechanisms going towards ICT infrastructure and to address digital divides
Global Agendas & Standards	<ul style="list-style-type: none"> • Develop rights-based policy and standards proposals relevant to global forums • Build stronger alliances and regional approaches to influence the ITU, 3GPP, and other standards bodies

Figure 8: Potential Entry Points for Engagement

Recommendations for Further Research

How Future Internet technologies are created, defined, governed, and used will have an impact on the future of data and information ecosystems and the choice between models of digital democracy and digital authoritarianism. Lessons from the parallel progression from 3G to 4G and concurrent rise in digital suppression and disinformation to undermine human rights can inform what to expect of the Future Internet. The importance of 5G goes beyond protecting democracy from equipment produced by companies close to the Chinese government. More robust action from democratic actors is required on 5G adoption and standards-setting to protect against rapidly evolving technology exploited by illiberal influencers. The existing critical risks associated with AI, data flow, and the Internet of Things are still widely overlooked but will be further underpinned by the transition to 5G. As countries vary in political context and development stages of 5G adoption, the democracy community needs to better understand and craft strategies to counter growing digital authoritarian trends across regions, in democracies and non-democracies alike. The current focus on economics and cybersecurity fails to capture some of the most pressing digital risk posed by illiberal 5G influence to human rights and democracy.

A central question for democracies is whether, and if so how, successful democracies can be maintained and strengthened in an ever-changing Internet-of-Everything era. More research is also needed into the digital strategic approach and partnerships, domestically and abroad, that will enable civil society, government, and stakeholders to effectively exercise oversight, and influence governance policies and decision-making forums. The implementation of humane, secure and customized technology standards and approaches is a priority. Big tech and local companies are playing a key role in complying with illiberal abuses of technology. Strategies are needed to effectively engage companies to be accountable and to understand that they too have an economic and social stake in secure networks.

The direct risks of 5G to democracy and human rights, and how best to frame technology policies, regulations, federal laws, and global standards to protect these rights must be more deeply understood in order to empower policymakers to understand the impact of their decisions. For instance, the risk of cybersecurity attacks on 5G-backed critical infrastructures like water utilities and power could potentially have significant repercussions for certain communities but are not often well understood or explained. Parliaments in particular don't have strong mechanisms for understanding the tradeoffs between digital convenience and democracy and individual rights.

NDI will take steps to begin addressing these problems. This research will inform ongoing NDI work. In addition, a primer will be adapted to assist policymakers in understanding some of the key challenges addressed above. Finally, NDI will work to promote these concepts and elevate the level of importance among policy leaders and the thought leadership community.

Acknowledgments

The authors owe a debt of gratitude to all of the experts who shared their knowledge with us throughout the development of this paper. We would like to thank Daniel Bagge, Jared Carlson, Steven Feldstein, Theo Jaekel, Berta Jarosova, Heather Johnson, Karolina Mensikova, Ugonma Nwankwo, Nicole Turner-Lee, and Eleanor Sarpong for sharing their time and thoughts with us.

We would also like to express thanks for the colleagues at NDI for their contributions to this project. Special thanks go to Manpreet Singh Anand, Summer Boucher-Robinson, Grant Godfrey, Peter Mattis, Sarah Moulton, Adam Nelson, Jim O'Brien, Dickson Omodi, Maggie Mitchell Salem, Kristen Sample, and Victoria Welborn.

References

- ¹ Global Mobile Suppliers Association. (January 2020). ["5G Market Status: Snapshot"](#). GSA Market.
- ² Osio, J.; Keith, E. (September 2020). ["52 Markets Worldwide With Commercial 5G Services"](#). S&P Global.
- ³ Sarpong, E. (April 2019). ["5G is Here! Can it deliver on Affordable Access?"](#). World Wide Web Foundation.
- ⁴ Davidson, Adam (October 2017). ["A Washing Machine that Tells the Future."](#) The Atlantic.
- ⁵ Lee, K.; Et. al. (October 2020). ["Digital Entanglement: China's Growing Digital Footprint in South Korea"](#). CNAS.
- ⁶ Ericsson. (March 2021). ["5G Human Rights Assessment"](#). Ericsson, Corporate Social Responsibility Report.
- ⁷ Linder, P. (July 2020). ["Putting the Spotlight on 5G in Rural Areas"](#). Ericsson.
- ⁸ UN Report. (May 2018). ["68% of the World Population Projected to Live in Urban Areas"](#).
- ⁹ ITU Report. (November 2019). ["Bridging the Gender Divide"](#). International Telecommunication Union.
- ¹⁰ ITU Press Release. (November 2019) ["Growing Internet Uptake But a Widening Digital Gender Divide"](#). ITU.
- ¹¹ GSMA. (2020). ["Global Report: The Mobile Economy"](#). GSMA.
- ¹² Sarpong, E. (April 2019). World Wide Web Foundation.
- ¹³ FP Analytics. (February 2020). ["5G Explained"](#). Foreign Policy Magazine.
- ¹⁴ Repucci, S. (2020). ["Freedom in the World 2020: A Leaderless Struggle for Democracy"](#). Freedom House.
- ¹⁵ Feldstein, S. (February 2020). ["When it Comes to Digital Authoritarianism"](#). Texas National Security Review.
- ¹⁶ Freyburg, T.; Garbe, L. (2018). ["Internet Shutdowns and Ownership at Election Times"](#). Open Technology Fund.
- ¹⁷ Parkinson, J.; Et al. (August 2019). ["Huawei Technicians Helped African Governments Spy"](#). Wall Street Journal.
- ¹⁸ Marczak, B.; Et al. (December 2020). ["Running in Circles"](#). The Citizen Lab, University of Toronto.
- ¹⁹ Kharpal, A. (March 2019). ["Huawei Says It'd Never Hand Data to China. But it Wouldn't Have a Choice"](#). CNBC.
- ²⁰ Savelii, S.; Applegate, M. (March 2021). ["Risks of Rushing to Internet Voting in Ukraine"](#). Atlantic Council.
- ²¹ Mozur, P. (April 2019). ["One Month, 500,000 Face Scans: How China Is Using A.I. to Profile"](#). New York Times.
- ²² Feldstein, S. (September 2019). ["The Global Expansion of AI Surveillance"](#). Carnegie.
- ²³ Bandeira, L.; Et al. (March 2019). ["Disinformation in Democracies"](#). Atlantic Council.
- ²⁴ Gorman, L. (October 2020). ["A Future Internet for Democracies"](#). German Marshall Fund.
- ²⁵ Polyakova, A.; Et al. (August 2019). ["Exporting Digital Authoritarianism: Russian and Chinese Models"](#). Brookings.
- ²⁶ Gorman, L. (October 2020). German Marshall Fund.
- ²⁷ Coredell, K. (December 2020). ["The ITU: The Most Important UN Agency You Have Never Heard Of"](#). CSIS.
- ²⁸ Kaspar, L.; Wingfield, R. (February 2021). ["Digital Rights at a Crossroads"](#). Global Partners Digital.
- ²⁹ Hillman, J. (March 2020). ["Beijing's Promotion of Alternative Global Norms and Standards"](#). CSIS.
- ³⁰ Gilbert, D. (December 2019). ["Zimbabwe Is Trying to Build a China Style Surveillance State"](#). Vice News.
- ³¹ Polyakova, A.; Et al. (August 2019). Brookings.
- ³² Grace, R. (August 2020). ["5G adoption and Its Implications in the Gulf States"](#). Middle East Institute.
- ³³ Woodhams, S. (August 2019). ["Digital Authoritarianism Rising in the Middle East"](#). Foreign Policy in Focus.
- ³⁴ Brown, H. (October 2019). ["Microsoft is Helping Israel Surveil Palestinians"](#). Vox News.
- ³⁵ Sen, S. (September 2020). ["India's Alliance With Israel Is a Model for the World's Illiberal Leaders"](#). Foreign Policy.
- ³⁶ Masih, N.; Et al. (December 2019). ["India's Internet Shutdown Longest Ever in Democracy"](#). Washington Post.
- ³⁷ Glick, B. (September 2020). ["Remarks on US-India-Israel Relations"](#). U.S. Agency for International Development.
- ³⁸ Arbel, T. (April 2021). ["Broadband for All: Inside President Biden's \\$100 Billion Plan"](#). Associated Press.
- ³⁹ Ericsson. (May 2018). ["Nordic Prime Ministers Unite to Prioritize 5G and Digitalization"](#). Ericsson News.
- ⁴⁰ Prague 5G Security Conference. (May 2019). ["The Prague Proposals"](#). Government of the Czech Republic.
- ⁴¹ Hemmings, J. (July 2020). ["South Korea's Growing 5G Dilemma"](#). CSIS.
- ⁴² Shah, R. (September 2020). ["Ensuring a Trusted 5G Ecosystem"](#). Australian Strategic Policy Institute.
- ⁴³ Galal, H.; Et al. (January 2020). ["5G: Creating New Value Across Industries and Society"](#). World Economic Forum, PwC.
- ⁴⁴ Farley, A. (August 2020). ["The Computer Scientist and Activist Who Got Big Tech to Stand Down"](#). Fast Company.