Author

Michel Girard

Senior Fellow, Centre for International Governance Innovation

Standards for a Secure 5G Infrastructure

5G BEYOND BORDERS

Acknowledgments

Cover image: Shutterstock/ By metamorworks

Key Points:

- There is an opportunity for governments and industry in North America to adopt common standards covering fifth-generation (5G) networks and Internet of Things (IoT) connected devices.

- To create a new 5G manufacturing ecosystem, participants in a North American Technology Trust need common interoperability standards.

- Developing a 5G technology road map will help to set priorities and identify gaps in standardization.

- 5G infrastructure should meet stringent security, health and safety standards. Governments and industry would benefit by jointly developing a "5G safety code" that sets the bar regarding security, health and safety requirements.

Introduction

5G infrastructure, composed of 5G networks and billions of IoT connected devices, is slated to become the backbone of the new digital economy. This policy brief is a contribution to a workshop focusing on the future of 5G in North America. The 5G Beyond Borders workshop, organized by the Wilson Center, CIGI and Tecnológico de Monterrey, aims to "discuss how strategic cooperation at the North American level can directly shape the future of 5G and lay the groundwork for expanded North American competitiveness in a range of emerging technologies."

The focus of the policy brief is on standardization. It explores how a North American Technology Trust can spur the development of standards that industry and governments need in order to build, maintain and operate a safe and reliable 5G infrastructure.

What Standards Are and Why They Matter

Although not visible to the average consumer, standards keep the economy running. They cover everything from the size of the simplest screw thread to the most complex information technology network. Standards provide a level playing field for industry and help build trust between participants in supply chains. They serve as a "handshake" between various components of systems and allow for interoperability. Standards also play a pivotal role in protecting health and safety in a wide range of sectors, including food and consumer products, infrastructure and the workplace. They are drafted in a way that allows another party to test and certify that a product, process or system meets the requirements of a specific standard. Put simply, standards make things work, help innovations spread and facilitate efficient trade nationally, regionally and internationally.

Many standards bodies were created at the beginning of the twentieth century to support industrialization. After World War II, new international organizations such as the International Organization for Standardization were established as trade liberalization discussions were gaining traction. Today, thousands of standards development organizations (SDOs) are managing more than one million national standards and more than 330,000 international standards (Girard 2018). Regarding 5G networks and connected devices, there are hundreds of SDOs and consortia involved in the development of standards and specifications for telecommunications and related technologies.

In the past decade, China has made considerable efforts to influence international standards (Wilson 2020; Steiger and Donath 2020). It is now a major contender in international telecommunication standardization fora such as the International Telecommunications Union (ITU) and the 3rd Generation Partnership Project (3GPP) consortium. Many observers note that China's growing clout in international standards development is accompanied by the adoption of divergent domestic standards. Different and conflicting requirements in national standards are interpreted as a way for the Chinese government to protect its domestic market from global competition. The strategy, dubbed "two markets, two resources," aims at the unilateral protection of the domestic market and the strategic exploitation of external ones through standards and certification programs (de La Bruyère and Picarsic 2020).

In response to China's two-pronged standards strategy, North America needs to forge a common view on standards for 5G infrastructure, and it needs to design and execute a winning standards strategy to achieve its objectives. To be

successful in creating a viable 5G manufacturing sector, governments and industry will need to identify what standards are required, make decisions regarding the adoption of international standards and invest in the development of regional standards when necessary. Additionally, governments and industry must deal with security, health and safety issues associated with the deployment of 5G.

Rationale for a North American Technology Trust

The rationale for the development of a North American approach to 5G was proposed in a recent paper by Meg King and Jake Rosen. With the ratification of the Canada-United States-Mexico Agreement (CUSMA), there is an opportunity for Canada, Mexico and the United States to "address the risks of untested technologies while simultaneously fostering innovation" (Wilson Center, n.d.). King and Rosen propose the creation of a North American Technology Trust as a way to shape the nature and character of emerging technologies, in response to China's emergence as a global leader in key technology disciplines (King and Rosen 2019, 2).

5G has emerged as one of the most important strategic areas of international technology competition, from an economic and a national security perspective. China is now seen by many as a threat to the security of democratic nation-states (Rodrik 2020). Recent reports from US officials state that telecommunications hardware manufacturer Huawei maintains backdoors to access sensitive and personal information in systems it builds and maintains around the world (Brandom 2020). Huawei is now the world's largest manufacturer of 5G network equipment and services. 5G networks and IoT connected devices could be used by foreign powers to collect data from users without their consent. 5G network equipment manufacturers could cripple networks over time by deliberately delaying important upgrades or by disabling them through hacking attacks.

As a response to economic and security threats, the governments of Canada, Mexico and the United States could join private sector partners in a North American Technology Trust and help create a seamless 5G network connecting almost 500 million users. With the right rules, standards and incentives in place, one could see the re-emergence of a vibrant North American telecommunications ecosystem encompassing research, testbeds and manufacturing. This could be done by developing a 5G technology road map and by devising a North American standardization strategy. In addition, the North American Technology Trust could help create a 5G safety code in order to tackle security threats and address growing health and safety issues.

Technology Road Map and Standardization Strategy

As indicated above, to be successful in creating a viable 5G manufacturing ecosystem, a North American Technology Trust would benefit from a technology road map. The road-map process has been used in North America to develop and deploy technologies such as semiconductors, the smart grid, cloud computing and military applications. Technology road maps can also help identify standardization "building blocks." Although progress has been made by international SDOs such as 3GPP to develop standards focused on spectrum allocation, much remains to be done to standardize core components of new wireless communications technologies.

This is why the Institute of Electrical and Electronics Engineers (IEEE) recently initiated a "5G and Beyond" technology road-map process. The IEEE, a leading international standards development organization, is headquartered in the United States. The IEEE initiative, entitled the International Network Generations Roadmap, covers 5G networks, connected devices and associated technologies over short- (three-year), medium- (five-year) and long-term (10-year) horizons (IEEE 2019a). It also aims to include linkages to emerging sixth-generation (6G) technologies. Fifteen working groups have been created to cover topics such as applications and services, edge automation platforms, hardware, spectrum, massive multiple input/multiple output antennas, mmWave and signal processing, optics, satellite, security, standards and testbeds. The road-map process would be kept evergreen to constantly adjust as new products and services emerge (IEEE 2020).

By contributing to the IEEE technology road-map process, a North American Technology Trust could identify key North American players able to participate in a new North American 5G manufacturing ecosystem operating with one set of interoperability standards. Today's telecommunications equipment industry is global in scope. It has been described as an "oligopoly of proprietary equipment vendors increasingly dominated by Huawei" (Rasser and Riikonen 2020). There are only three non-Chinese suppliers of 5G equipment: Nokia of Finland, Ericsson of Sweden and Samsung of South Korea. As a result of industry consolidation in the 1990s and 2000s, foreign firms acquired large US-based players including Lucent, Alcatel and Motorola. In Canada, Nortel Networks ceased operations more than 10 years ago. To make matters more complex, there is in parallel a rapidly growing number of IoT devices vendors and suppliers entering the market, many of which are based outside North America. Billions of devices are expected to use 5G networks to support new applications such as smart homes, telemedicine, industry 4.0, networked agriculture and self-driving cars. Active participation of governments and industry in the technology road-map process would help identify anchor firms that have the capacity to manufacture and maintain a wide array of 5G-related equipment and encourage innovative companies in emerging sectors to join the North American Technology Trust.

As part of the technology road-map process, the IEEE is also spearheading a review of the 5G standardization landscape. In a recent report entitled *Standardization Building Blocks*, the working group aims to illustrate a master timeline for the standardization of wireless communications technologies and map out the relevant SDOs and consortia involved in the sector, the interactions between organizations and the touch points between standards. Core technology standards are currently developed by the IEEE along with more than 65 SDOs, consortia and industry alliances

as well as six open-source organizations. However, a number of new players have begun to map out 6G applications, which would ideally be integrated with existing networks to maintain interoperability (IEEE 2019b).

As part of their deliberations on standards, participants in the North American Technology Trust could also investigate the merits of new approaches to build and maintain 5G infrastructure. The market is currently dominated by service providers using proprietary solutions to manufacture non-interoperable equipment. Different approaches could foster more competition, increase innovation and possibly lower the price of 5G equipment. Open radio access networks (RAN) is one approach that is gaining traction. It aims at creating open standards to spur the manufacturing of 5G modular equipment with open interfaces, allowing for interoperability of equipment across multiple vendors and supply-chain diversity. Standardization of security can be applied to supply chain participants, and systems can be designed to allow for end-to-end encryption (O-RAN, n.d.).

Depending on the standards paths pursued, the North American Technology Trust may need to develop its own copyright, intellectual property and patent strategy. Individual industry protection will be required for owners of essential patents in standards. Perhaps patent pools, which are agreements between various patent owners to license their patents to one another or to third parties, could be considered in order to create winning partnerships and supply chains.

With a robust 5G technology road map, the Technology Trust will be in a position to design a suitable standardization strategy. It would map out what standards are being developed nationally, regionally and internationally and outline how to successfully engage in international standardization bodies. For example, US industry participation in international SDOs such as the ITU has declined over time, leaving scope for China to lead. Many international standardization experts have urged US authorities and US industry to strategize on how best to re-engage these fora. For example, stakeholders engaged in the 3GPP are in the process of reforming rules to ensure that China's participation in technical committees and working groups does not overwhelm other interests. A similar process could be considered with regard to the ITU, which is accountable for critical 5G telecommunication standards.

Standardization gaps can also be addressed in the strategy. A critical success factor will be for participants in each North American jurisdiction to develop a common view on 5G standards and to implement its standardization strategy in a coordinated way. The need for regional dialogues and strategic discussions on standardization in other sectors has led to the creation of broad-based regional coordination bodies such as the Pan American Standards Commission, the Pacific Area Standards Congress and the Council for Harmonization of Electrotechnical Standards of the Nations of the Americas. In Europe, the European Committee for Standardization and the European Committee for Electrotechnical Standardization coordinate standardization activities for the European Commission with the assistance of national standards bodies in participating jurisdictions. Perhaps enhancing coordination on 5G standardization issues between Canada, Mexico and the United States could be explored under the regulatory cooperation chapter of CUSMA.

5G Safety Code

In addition to technology and interoperability requirements, governments and industry should also set a bar regarding the overall security of the 5G network and connected devices (Wiley Law 2021). Perhaps the most important issue to address is the development and adoption of enforceable cybersecurity standards. New standards are needed to

ensure that the data carried by 5G infrastructure as a whole is safe from unauthorized access and that IoT, transmission and routing devices can withstand intrusion, manipulation and hacking (Council on Foreign Relations 2020). 4G networks are less vulnerable to intrusions as there is a clear demarcation between core networks and RAN at the edge.

With 5G, however, the core and the edge are blended. Much of the core's traditional functions under 4G will be pushed to the edge "to reduce latency: speeding up communication to enable new functionalities such as autonomous vehicles and telemedicine, where a millisecond lag can be a matter of life and death" (Rasser and Riikonen 2020, 6). The 5G architecture will need to be secured seamlessly as many components in the chain are currently not designed with cybersecurity in mind (Girard 2020). Ideally, governments in the three participating jurisdictions would agree to work with industry on standards that outline minimum requirements covering emission security, physical security, transmission security and cryptographic security.

Emerging health and safety concerns associated with 5G towers and other transmission equipment will need to be addressed as well. There is a growing number of incidents involving public protests and acts of sabotage around the world, sometimes fed by online conspiracy theories and dubious science (DW 2020; Radiation Dangers 2020; Daalder 2020). These concerns cannot be ignored. Without a social licence to operate, efforts to deploy 5G networks could be thwarted. Standards asserting acceptable health and safety requirements for 5G transmission equipment for users as well as for workers in the industry would help alleviate these concerns. The standards development process is inclusive and encourages the participation of interested stakeholders in technical committees and working groups including industry, regulators, academics, experts and consumers. Third-party certification of equipment to stringent performance standards could change the dynamics of the debates around the safety of 5G transmission equipment.

Participants in the North American Technology Trust could work together and spur the development of a 5G safety code. Safety codes are defined as a series of rules and objectives applying to a particular sector. They cover installation and maintenance of products and infrastructure in a wide range of sectors including electrical, plumbing, oil, gas, buildings and communications infrastructure. Most of these safety codes have been put in place since the 1950s to protect users, workers, nearby residents and the environment. In Canada, these normative documents are often incorporated by reference in regulations. In the United States, they are generally used as a self-regulation mechanism but have proven effective in keeping consumer products and infrastructure safe and reliable.

Looking Forward

In this policy brief, the author argues that the proposed North American Technology Trust could spur the emergence of a vibrant 5G manufacturing ecosystem, provided that governments and industry work closely together and come up with both a solid standardization strategy and a credible 5G safety code. But time is of the essence. Beijing is about to release its China Standards 2035 strategy. It will likely outline how the IoT, 5G and artificial intelligence will be standardized into a seamless web. Looking forward, Canada should expect that China will further increase its engagement in standards setting nationally, regionally and internationally. In the words of the Standardization Administration of China, third-tier companies do products, second-tier companies do technologies and first-class companies do standards. It is now up to North America to take up the challenge.

Works Cited

Brandom, Russell. 2020. "Feds claim Huawei can snoop on mobile networks." The Verge, February 11.
www.theverge.com/2020/2/11/21133631/huawei-china-spying-claims-us-officials-blacklist-5g.

Council on Foreign Relations. 2020. "The State of U.S. 5G." Council on Foreign Relations, Virtual Meeting, July 14.
www.cfr.org/event/virtual-meeting-state-us-5g.

Daalder, Marc. 2020. "Cell towers targeted as 5G conspiracy theory spreads." Stuff, April 9.
www.stuff.co.nz/technology/120941014/cell-towers-targeted-as-5g-conspiracy-theory-spreads.

De La Bruyère, Emily and Nathan Picarsic. 2020. *China Standards 2035: Beijing's Platform Geopolitics and "Standardization Work in 2020."*
Horizon Advisory China Standards Series.

DW. 2020. "5G protesters sabotage Dutch phone towers." DW, April 11.
www.dw.com/en/5g-protesters-sabotage-dutch-phone-towers/a-53094033.

Girard, Michel. 2018. "Canada Needs Standards to Support Big Data Analytics." Policy Brief No. 145, Centre for International Governance
Innovation, December 4. www.cigionline.org/publications/canada-needs-standards-support-big-data-analytics.

———. 2020. "Standards for Cybersecure IoT Devices: A Way Forward." Policy Brief No. 160, Centre for International Governance Innovation,
July 15. www.cigionline.org/publications/standards-cybersecure-iot-devices-way-forward.

IEEE. 2019a. "International Network Generations Roadmap (INGR): An IEEE 5G and Beyond Technology Roadmap — Executive Summary."
1st Edition. IEEE. https://futurenetworks.ieee.org/images/files/images/roadmap/INGR_ExecSumm_Ed1.pdf.

———. 2019b. "International Network Generations Roadmap (INGR): An IEEE 5G and Beyond Technology Roadmap — Standardization Building
Blocks." 1st Edition. IEEE.

———. 2020. "IEEE 5G and Beyond Technology Roadmap White Paper." IEEE.
https://futurenetworks.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf.

King, Meg and Jake Rosen. 2019. "Building a North American Technology Trust." *Yale Journal of International Affairs* 14: 1–12.

Nyczepir, Dave. 2020. "White House, Pentagon agree to fastest transfer of spectrum for commercial 5G use." Fedscoop, August 10.
www.fedscoop.com/pentagon-spectrum-transfer-5g/.

O-RAN. n.d. "O-RAN ALLIANCE is Transforming the Radio Access Networks Industry Towards Open, Intelligent, Virtualized and Fully Interoperable
RAN." www.o-ran.org/.

Radiation Dangers. 2020. "Study Shows Direct Correlation between 5G Networks and 'Coronavirus' Outbreaks." Radiation Dangers, April 24.
http://radiationdangers.com/5g/study-shows-direct-correlation-between-5g-networks-and-coronavirus-outbreaks-2/.

Rasser, Martijn and Ainikki Riikonen. 2020. *Open Future: The Way Forward on 5G*. Washington, DC: Center for a New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Open-Future-The-Way-Forward-on-5G-final1-min.pdf?mtime=20200811091437&focal=none.

Rodrik, Dani. 2020. "The Coming Global Technology Fracture." Project Syndicate, September 8. www.project-syndicate.org/commentary/making-global-trade-rules-fit-for-technology-by-dani-rodrik-2020-09.

Steiger, Gerhard and Steffen Donath. 2020. "New standardization strategy 'China Standards 2035.'" ETMM Online, August 25. www.etmm-online.com/new-standardistion-strategy-china-standards-2035-a-958253/.

Wiley Law. 2021. *5G and Government: A Regulatory Roadmap*. Washington, DC: Wiley Rein LLP. www.wiley.law/media/handbook/550_2021-Wiley-5G-Roadmap.pdf.

Wilson Center. n.d. "5G." www.wilsoncenter.org/issue/5g.

Wilson, Naomi. 2020. "A 'China Model?' Beijing's Promotion of Alternative Global Norms and Standards." Testimony before the U.S.-China Economic and Security Review Commission, Washington, DC, March 13. www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Naomi%20Wilson%20ITI.pdf.

About the Author

Michel Girard is a senior fellow at CIGI, where he contributes expertise in the area of standards for big data and artificial intelligence (AI). His research strives to drive dialogue on what standards are, why they matter in these emerging sectors of the economy, and how to incorporate them into regulatory and procurement frameworks. He highlights issues that should be examined in the design of new technical standards governing big data and AI in order to spur innovation while also respecting privacy, security and ethical considerations.

In addition, Michel provides standardization advice to help innovative companies in their efforts to access international markets. He contributes to the CIO Strategy Council's standardization activities and advises the Chartered Professional Accountants of Canada on data governance issues.

Michel has 22 years of experience as an executive in the public and not-for-profit sectors. Prior to joining CIGI, Michel was vice president, strategy at the Standards Council of Canada (SCC), where he worked from 2009 to 2018. At the SCC, he led the design and implementation of the Standards and Innovation program, the Climate Ready infrastructure program, the Northern Infrastructure Standards Initiative and the Monitoring Standards in Canadian Regulations project. He managed the negotiation of standardization clauses in trade agreements including the Comprehensive Economic and Trade Agreement and the Canadian Free Trade Agreement. Previously, he was director of the Ottawa office at the Canadian Standards Association, director of international affairs at Environment Canada, corporate secretary at Agriculture Canada and acting director of education and compliance at the Canadian Environmental Assessment Agency. He holds a Ph.D. and a master's degree in history from the University of Ottawa.

About the Project: 5G Beyond Borders

5g.wilsoncenter.org

The **Wilson Center's 5G Beyond Borders** project explores how the U.S., Canada, and Mexico can work together to maximize the benefits of 5G and related technology through informed policy solutions. The project offers an overview of the landscape of 5G technology around the globe, while also focusing on the impact of 5G on North American business, and smart manufacturing. Cross-border collaboration between the U.S., Canada, and Mexico is essential to a secure transition. 5G Beyond Borders explores not only 5G security, but how North American cooperation can reduce risks, maximize economic gains, and ensure an efficient 5G rollout.

Workshop Partners

The Wilson Center was chartered by Congress in 1968 as the official memorial to President Woodrow Wilson. It serves as the nation's key non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community. The workshop is part of the Wilson Center's **5G Beyond Borders** project, which is a larger collaboration between the Wilson Center's Mexico Institute, Canada Institute, and Science and Technology Innovation Program (STIP).

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Tecnológico de Monterrey is a private, non-profit, and independent institution with no political and religious affiliations, founded in September of 1943. Since then, the university has enrolled more than 65,000 undergraduate and graduate students in Monterrey, Mexico City, Guadalajara and 26 other cities in Mexico. The work of Tecnológico de Monterrey is supported by civil associations made up of a numerous group of outstanding leaders from all over the country who are committed to quality in higher education. It is the only non-US university in the Princeton Review of Top Schools for Entrepreneurship Studies (2020).

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

⊕ www.wilsoncenter.org

✉ wwics@wilsoncenter.org

f facebook.com/woodrowwilsoncenter

🐦 @thewilsoncenter

《📱》 202.691.4000

Wilson Center