Instituto de Tecnologia & Sociedade do Rio

Managing 5G Security Challenges: Options for Multistakeholder Governance

Amy Ertan
Royal Holloway, University of London
Information Security Group

Christian Perrone
LL.M. Cantab - Fulbright Fellow
Institute for Technology and Society, Rio de Janeiro

Abstract

This article highlights current security challenges relating to 5G deployment and explores the opportunities of appropriate and applicable governance mechanisms. Through the analysis of current security concerns around supply chain provision of the technology via Huawei, the article outlines the need for comprehensive governance which considers both technical and geopolitical security matters. This research explores the different options for governance for 5G security and argues that a multistakeholder approach offers the most productive opportunity for effective oversight and decision-making. Through a case study on CGI.br and internet governance, this research highlights how multistakeholder governance approaches can be effective in practice.

Introduction

The emergence of fifth-generation wireless technology - 5G - offers opportunities through vastly improved interconnectivity across different environments, from smart cities (autonomous transport, intelligent power grids and energy plants) to technology within the private sphere of the home (including internet of things devices such as smart locks, surveillance systems and even banal kitchen appliances). With the potential to facilitate exponentially faster information transfer than 5G's predecessors, significant tensions are observable across states as governments seek to manage implementation and governance processes over a technology that is expected to form a significant part of core infrastructure within the next few years. As one example, telecommunications infrastructure will rely heavily on 5G deployment, which in turn provides the basis of much of the digital economy and operations at the state level. This paper will explore how states approach the challenge of maintaining control of core sovereign decision-making, and secure the confidentiality, integrity and availability of sensitive data, with a technology that has been developed by technical bodies and the private sector.

The first section of this paper highlights the main security concerns around 5G technology, reviewing the current 5G landscape as well as the expectations for the near-future proliferation of internet connectivity that 5G technology will offer. From the expanded cyber-attack vector due

to the increased number of internet-connected devices[1], to the increased privacy risks to the user[2], this section considers the inherent complexities involved in the implementation and governance of 5G infrastructure.

Through the use of a case study, the second section of this paper refers to the ongoing debates surrounding Chinese technology company Huawei, and the decisions of several state governments to limit Huawei's role as a supplier of 5G in critical national infrastructures. As well as analysing the geopolitical tensions that were exacerbated by 5G supplier considerations, this discussion also provides a context around the need to understand cybersecurity concerns relating to 5G.

Having introduced the range of challenges that complicate both the deployment, maintenance and governance of 5G technology, the third section introduces the need for multistakeholder governance concerning the cybersecurity landscape and the implementation of 5G. Following an outline of the most relevant cybersecurity considerations when it comes to 5G roll-out, this paper outlines the necessity of robust implementation management and responsible governance and showcases the challenges and opportunities of collaborative multistakeholder models.

The fourth and final section of this paper discusses the Brazilian internet governance model - particularly, the Brazilian Internet Steering Committee - CGI.br - to illustrate how multistakeholder governance of cyber-related activity can be inclusive, open and effective. A comparative analysis enables this paper to explore the challenges and opportunities in transposing such models onto the emerging 5G technology landscape.

This paper draws multidisciplinary principles from fields including law, political science, organisational management and information security, to argue that multistakeholder governance is essential for the responsible and inclusive implementation of a new era of internet-connected living.

I. 5G and Cybersecurity

> *"This is a matter of security — of national security — because the 5G network is not just the next communications network; it is where our entire lives will be located in the future…..It is where cars will drive, where surgeons will perform*

---

[1] Tiburski, Ramão Tiago, Leonardo Albernaz Amaral, and Fabiano Hessel. "Security Challenges in 5G-Based IoT Middleware Systems." In *Internet of Things (IoT) in 5G Mobile Technologies*, pp. 399-418. Springer, Cham, 2016.

[2] Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. "5G security: Analysis of threats and solutions." In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193-199. IEEE, 2017.

> *surgeries, where factories will operate. Our entire lives will be on there. This is not just a matter of a network."*[3]
>
> - *Sven Sakkov, Director of the International Centre for Defence and Security (Estonia)*

5G technology offers transformative effects across modern-day life. From core national infrastructure to the connectivity offered to individual users on their mobile devices, 5G security has been an area of active research across industry, academia, nonprofits and state actors. 5G security vulnerabilities arise both through the expansion of existing threats (as more insecure devices become connected to the internet, for example), and through the expectation of new threats impacting 5G technology and its equipment (for example, the increased capability of surveillance as a potential challenge to user privacy). This section offers an overview of security challenges, highlighted across the technical and strategic literature, and argues that challenges come in many forms, including and not limited to technological, economic, standards-based, geopolitical (especially relating to critical national infrastructure), and privacy challenges. Effective governance of 5G technology requires an understanding of these aspects in context, and integration of all relative stakeholders when designing governance structures.

1.1 Technical Security Challenges[4]

Academic literature has highlighted the following key technical security challenges: 5G Architecture relies on several new technology concepts, such as Software-Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing, which hold challenges relating to privacy and potential vulnerabilities.[5] Existing research has outlined the need for a robust technical security architecture for 5G networks with technical solutions.[6]

---

[3] Vahtla, Aili, ed. "ICDS Director: 5G Memorandum a Matter of Security for Estonia." *ERR*, October 29, 2019. Retrieved from http://web.archive.org/web/20200622011001/https://news.err.ee/997106/icds-director-5g-memorandum-a-matter-of-security-for-estonia.

[4] There are a huge range of technical cybersecurity challenges that we recognise but will not focus on in this paper, for the reason that they are not necessarily addressed by governance and state policy, but through active technical research. For an overview of technical challenges with 5G, please refer to: Ahmad, Ijaz, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, and Mika Ylianttila. "Security for 5G and beyond." *IEEE Communications Surveys & Tutorials* 21, no. 4 (2019): 3682-3722.

[5] See also Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. "5G security: Analysis of threats and solutions." In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193-199. IEEE, 2017; Liyanage, Madhusanka, Jukka Salo, An Braeken, Tanesh Kumar, Suranga Seneviratne, and Mika Ylianttila. "5G privacy: Scenarios and solutions." In *2018 IEEE 5G World Forum (5GWF)*, pp. 197-203. IEEE, 2018

[6] Schneider, Peter, and Günther Horn. "Towards 5G security." In *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 1165-1170. IEEE, 2015.

For example, one consequence of the increasing connectivity opportunities offered by 5G is expected to contribute to the 'disruptive' proliferation of Internet-of-Things (IoT) devices.[7] IoT security is an intensely active area of information security research, from the security of end-point devices, particularly as research has highlighted high rates of insecure devices.[8] From webcams and smart locks to smart fridges and energy monitoring systems, devices with no default passwords, or with poor security configurations, may be easily compromised. This poses a security risk through the data that is released (or through direct malicious action, such as interfering with smart-lock settings). The rise in connected devices also allows the creation of huge 'botnets' (collections of compromised or unsecured IoT devices) by malicious actors, to carry out distributed 'denial of service attacks' (when a victim's network is overloaded with malicious traffic),[9] a trend already observed from 2016 through prominent IoT botnets such as Mirai.[10] In a clear sense, 5G technology amplifies many of the security challenges relating to IoT security as a whole,[11] a field in which the challenge of inexpensive, poorly secured devices represent significant vulnerabilities against cyberattacks.[12]

It is important to note that technical security challenges may be pertinent throughout the entirety of the supply chain, from hardware manufacturers (for example, providers who design and build chipsets), to incorrect user configuration of 5G-enabled devices. When trying to mitigate or develop appropriate governance, excluding any part of the supply chain may increase relative risks as excluded stakeholders may develop insecure practices.[13] All parts of the supply chain have a part to play - as the cliche goes, the chain is only as strong as its weakest link.

---

[7] Palattella, Maria Rita, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel, and Latif Ladid. "Internet of things in the 5G era: Enablers, architecture, and business models." *IEEE Journal on Selected Areas in Communications* 34, no. 3 (2016): 510-527.

[8] Ahmad, Ijaz, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, and Andrei Gurtov. "Overview of 5G security challenges and solutions." *IEEE Communications Standards Magazine* 2, no. 1 (2018): 36-43.

[9] Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu. "Security for 5G mobile wireless networks." *IEEE Access* 6 (2017): 4850-4874.

[10] Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. "DDoS in the IoT: Mirai and other botnets." *Computer* 50, no. 7 (2017): 80-84

[11]'Internet of Things' security research is an incredibly active field of research. For an overview of recent research trends: Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." *Computer networks* 148 (2019): 283-294.

[12] Miloslavskaya, Natalia, and Alexander Tolstoy. "Internet of Things: information security challenges and solutions." *Cluster Computing* 22, no. 1 (2019): 103-119.

[13] "Secure by Design ." *Gov.UK*, Department for Digital, Culture, Media and Sport, 6 June 2019, Retrieved from web.archive.org/web/20200623144358/www.gov.uk/government/collections/secure-by-design.

1.2 Practical implementation challenges

There are several other challenges to consider with 5G which will inhibit the pace of deployment. As of 2020, the emerging technology is incredibly expensive to implement and maintain, relative to its predecessors.[14] Due to these costs, it is likely that 5G coverage will initially be focused on areas with highly-concentrated-populations, with rural areas likely to fall behind in terms of connectivity.[15] This narrow geographical focus is likely to be exacerbated by issues of latency;[16] while 5G provides significantly faster data transfer compared to its wireless predecessors, it is also impacted by physical barriers including walls and distance.[17]

1.3 Standards-based challenges - security implications

As well as governments and supplier organisations, there are several actors invested in the long term direction of 5G innovation, and this presents itself through attempts to develop appropriate standards for 5G innovation. Actors including the United Nations International Telecommunications Union help facilitate forums such as the World Telecommunications Conference (held every 3-4 years) where attending parties (mostly focused on State's points of view) develop standards, while the 3rd Generation Partnership Project (3GPP) tends to focus more on technical points of view brought by the main companies in the sector.[18] The National Institute for Standards and Technology (NIST) sponsors the '5G Millimeter-Wave (mmWave) Channel Model Alliance', a research consortium through which the output is expected to be incorporated into developed standards[19]. There are also huge sector-specific shifts which will depend on standards and associated regulation. For example, within telecommunications, mobile network operators ('MNO's) must transform the nature of their networks to meet the demands and challenges of 5G technology, and this is likely to require regulatory oversight on

---

[14] See Jones, Peter, and Daphne Comfort. "A commentary on the rollout of 5g mobile in the UK." *Journal of Public Affairs* 20, no. 1 (2020): e1993; Yardley, Matt, Janette Stewart, Ian Adkins, and Robert Woolfson. *Lowering Barriers to 5G Deployment*. July 2018. Report for the Broadband Stakeholder Group

[15] Oughton, Edward J., and Zoraida Frias. "The cost, coverage and rollout implications of 5G infrastructure in Britain." *Telecommunications Policy* 42, no. 8 (2018): 636-652.

[16] Parvez, Imtiaz, Ali Rahmati, Ismail Guvenc, Arif I. Sarwat, and Huaiyu Dai. "A survey on low latency towards 5G: RAN, core network and caching solutions." *IEEE Communications Surveys & Tutorials* 20, no. 4 (2018): 3098-3130.

[17] Mezzavilla, Marco, Menglei Zhang, Michele Polese, Russell Ford, Sourjya Dutta, Sundeep Rangan, and Michele Zorzi. "End-to-end simulation of 5G mmWave networks." *IEEE Communications Surveys & Tutorials* 20, no. 3 (2018): 2237-2263.

[18] 3GPP - A Global Partnership Retrived from https://web.archive.org/save/https://www.3gpp.org/dynareport/SpecList.htm?release=Rel-15&tech=4

[19] For more information on NIST's 5G alliance refer to "Alliance for 5G Networks." *NIST.gov*, 2020, http://web.archive.org/web/20191231020334/https://www.nist.gov/industry-impacts/alliance-5g-networks; "5G mmWave Channel Model Alliance"." *NIST.gov*, 2020, http://web.archive.org/web/20200623193141/https://www.nist.gov/ctl/5g-mmwave-channel-model-alliance.

competitive 'race to 5G'.[20] As of mid-2020, standards remain an ongoing effort. Research published by the European Parliament highlights the lack of finalised agreement on 5G standards as a potential dampener to realising the full benefits of 5G innovation.[21]

1.4 Privacy-based challenges

Research by Privacy International argues that the 'hyperconnected world' facilitated by 5G technology represents a challenge for privacy, in which improved network precision capabilities allow for easier identification of users.[22] 5G technologies have implications across several user privacy concepts, with improved connectivity across applications providing challenges for data, identity and location privacy.[23] With different stakeholders across the 5G supply chain, user data is expected to change hands many times, increasing the risks and reducing aspects of user control (and awareness) over how their data is used.[24]

1.5 Sector Focus: The Supply Chain and Critical National Infrastructure

Deploying 5G infrastructure - from communications masts to chipsets - relies on using specialised technology providers. This reliance on parties in the supply chain also raises various risks, including key concerns relating to cybersecurity. While the deployment of 5G technology across critical national infrastructure is likely to have accounted for the basic cyber-hygiene controls examined above (poor access control, for example), the confidentiality, availability and integrity (the triad of traditional cybersecurity concerns) of data? remain a key focus. The developers and distributors of 5G infrastructure in the telecommunications sector have the potential to access vast amounts of data, including access to sensitive and personally identifiable data. It is therefore essential that as governments look to roll out 5G across national infrastructure - and in particular critical national infrastructure like telecommunications - that the supplier is trusted to operate responsibly and transparently with regards to data privacy and cybersecurity concerns.

1.6 The 5G and cybersecurity innovation ecosystem

While this paper focuses on the governance challenges for managing overall 5G security concerns, the economic, administrative and technological challenges of implementation must

---

[20] Lehr, William. "Future of Broadband Competition in a 5G World." *Available at SSRN 3240191* (2018).

[21] Blackman, Colin, and Simon Forge. *5G deployment: State of play in Europe, USA and Asia*. European Parliament, 2019.

[22] "Welcome to 5G: Privacy and Security in a Hyperconnected World (or Not?)." *PrivacyInternational.org* (blog), July 23, 2019. http://web.archive.org/web/20200622021346/https://www.privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not.

[23] Liyanage, Madhusanka, Jukka Salo, An Braeken, Tanesh Kumar, Suranga Seneviratne, and Mika Ylianttila. "5G privacy: Scenarios and solutions." In *2018 IEEE 5G World Forum (5GWF)*, pp. 197-203. IEEE, 2018.

[24] *ibid.*

also be considered within an effective governance strategy. The search for potential solutions to 5G security challenges are a subject of interest for a huge range of actors, including researchers across academia. Many universities will have 5G research programmes,[25] and there are also several cross-sector initiatives attempting to draw together parts of the 5G ecosystem, including academia, start-ups, and major corporations.[26] The role of academia is active and integral,[27] particularly where research may not have an immediate or near-term return. Non-profits have also been active in this space, with reports highlighting the opportunities 5G technologies hold for society, but also considering pressing challenges, with think-tanks highlighting issues relating to sovereignty[28] and network security.[29] Faced with the broad, intersecting set of challenges facing 5G implementation and maintenance, coupled with the sheer breadth of activity to investigate and (attempt to) mitigate these challenges, understanding the swiftly shifting dynamics of 5G innovation is no simple feat. Attempts at 5G governance must take the diversity of activity and security concerns into consideration in order to develop an inclusive governance strategy. This will involve engaging many of the stakeholders mentioned above, determining actors of influence that may positively shape an effective governance model.

II. Challenges in Practice: Huawei and 5G

Having introduced the categories of security threats facing 5G technology, and stated the necessity of effective 5G governance and security, it is time to consider a prominent real-world example. When it comes to examining security and 5G infrastructure in practice, one central ongoing discussion is the wider geopolitical context, focusing on Huawei's place in national infrastructure supply chains.

2.1 Who is Huawei and why is its 5G involvement so contentious?

---

[25] A few examples in the UK alone include the University of Surrey's '5G Innovation Lab', Bristol University's 'Smart Internet Lab' and the 'Centre for Telecommunications Research' at King's College London all of whom have dedicated research teams looking at 5G security. For more information on the UK academic '5G hub' refer to http://web.archive.org/web/20200622005142/https://re.ukri.org/funding/our-funds-overview/uk-research-partnership-initiative-fund/case-studies/5g-innovation-centre-5gic-university-of-surrey/.

[26] One example of a cross-sector initiative is the Verizon Lab: https://web.archive.org/save/https://verizon5glabs.com

[27] Additionally search on https://scholar.google.com for '5G Security' returns 'about 91,500 results', with 'about 16,000 results' once the search is narrowed to include publications since 2019 . Of course this is by no means a perfect metric of activity, as many papers may include the terms as peripheral references, however the sheer number of results highlight the attention cited papers receive.

[28] 5G in Europe: Time to Change Gear! *Institute Montaine* Working paper. May 2019. http://web.archive.org/web/20200622030222/https://insightsforgood.mazars.com/wp-content/uploads/2019/06/5g.pdf.

[29] Rühlig, Tim, and Maja Björk. "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe." (2020).

Huawei is a Chinese multinational technology corporation, well-known for its development of mobile devices and telecommunications equipment. While the corporation describes itself as an 'employee-owned' company[30], research has highlighted extensive ties with the Chinese government[31] / PLA to the extent that Huawei 'may be deemed effectively state-owned'.[32] The corporation is widely considered to be a world-leading provider of 5G network technology[33], 'vying to amass 5G patents' alongside a relatively small number of corporations including Ericsson and Nokia.[34]

While all telecommunications providers must consider the technical challenges to 5G technology (described above), the primary concern around Huawei's involvement is the potential for surveillance access across telecommunications infrastructure, particularly where instructed and condoned by the Chinese government.[35] The threat of cyber-espionage, in which data is accessed and surveilled (and potentially stolen or manipulated), has been frequently reported in relation to Chinese activity.[36]

Within wider geopolitical and economic competition for technical superiority, the Chinese state holds several advantages due to established civil-industry fusion structures and a private-public partnership structure that forms a key part of Chinese technical innovation and cybersecurity strategies.[37] The former head of MI6 has referred to Huawei as a 'state-managed, quasi military enterprise' that forms part of Chinese 'economic colonialism', referring to the technical

---

[30] "Huawei Facts Q&A Who Owns Huawei?" Huawei.com. Retrieved from: https://web.archive.org/save/https://www.huawei.com/en/facts/question-answer/who-owns-huawei.

[31] Balding, Christopher, and Donald C. Clarke. "Who Owns Huawei?." *Available at SSRN 3372669* (2019).

[32] Corera, Gordon. "Eric Schmidt: Huawei Has Engaged in Unacceptable Practices." BBC, June 18, 2020. Retrieved from http://web.archive.org/web/20200619233649/https://www.bbc.com/news/technology-53080113.

[33] Curwen, Peter. "Huawei and goodbye." *Digital Policy, Regulation and Governance* (2020).

[34] Auchard, Eric, and Stephen Nellis. "What Is 5G and Who Are the Major Players?" *Reuters*, March 15, 2018. Retrieved from http://web.archive.org/web/20200621222645/https://www.reuters.com/article/us-qualcomm-m-a-broadcom-5g-idUSKCN1GR1IN

[35] Chapman, Ben. "Huawei: Why Are Western Governments Worried about China's Technology Powerhouse?" *Independent (UK)*, January 18, 2019. Accessed June 10, 2020. https://www.independent.co.uk/news/business/news/huawei-china-national-security-threat-arrests-technology-spying-espionage-a8734461.html.

[36] Hoffman, Samantha, and Elsa Kania. "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws." *The Strategist* 13 (2018).

[37] Kania, Elsa B. *Securing Our 5G Future: The Competitive Challenge and Considerations for US Policy*. Center for a New American Security., 2019.

superiority China holds in 5G innovation, and how this may be used to further political and economic aims.[38]

The intertwined and often unclear link between the Chinese-based industry and state infrastructure feeds into Western-states suspicions that Huawei and other Chinese firms may be vehicles for Chinese state surveillance. In strategic national security terms, this is a significant disincentive for foreign governments to contract Huawei to provide the core provision of 5G infrastructure.[39]

2.2 *Responding to challenges in the supply chain*

As of June 2020, states have imposed (and subsequently withdrawn) limitations of some shape and form on Huawei, with approaches varying by state. In April 2019, all five members of the intelligence network 'Five Eyes' (UK, US, Canada, Australia and New Zealand) had made commitments restricting Huawei to 'sensitive' parts of their telecoms networks, with Australia blanket-banning Huawei's participation in its national infrastructure,[40] and Britain restricting Huawei's access to core parts of 5G infrastructure.[41] Since then, many states have updated their public-facing statements on Huawei's involvement in the national roll-out of 5G technology. While as of early January 2020 Huawei was positioned to develop non-core parts of the UK's 5G infrastructure, in May 2020 domestic political pressure led to the UK government committing to reduce Huawei's involvement.[42] In direct response, Huawei launched targeted ads in several British news providers attempting to reassure the public of Huawei's 'role to help Britain lead the

---

[38] Elwes, Jay. "Former Head of MI6: Huawei Is a Threat to Britain "without Question"." *The Article*, January 15, 2020. Elwes, Jay. "Former Head of MI6: Huawei Is a Threat to Britain "without Question"." *The Article*, January 15, 2020. https://www.thearticle.com/former-head-of-mi6-huawei-is-a-threat-to-britain-without-question.

[39] Sullivan, James, and Rebecca Lucas. "5G Cyber Security A Risk-Management Approach." *RUSI Occasional Paper*, February 2020. Retrieved from http://web.archive.org/web/20200620022452/https://rusi.org/sites/default/files/20200602_5g_cyber_security_final_web_copy.pdf

[40] Remeikis, Amy. "China Accuses Australia of Discriminating against Huawei." *The Guardian*, February 17, 2020. Retrieved from http://web.archive.org/web/20200622164851/https://www.theguardian.com/australia-news/2020/feb/17/china-accuses-australia-of-discriminating-against-huawei.

[41] Holden, Michael, and Jack Stubbs. "Five Eyes Will Not Use Huawei in Sensitive Networks: Senior U.S. Official." *Reuters*, April 24, 2020. Retrieved from: http://web.archive.org/web/20200528014546/https://www.reuters.com/article/us-britain-huawei-ncsc-usa-idUSKCN1S01CZ.

[42] Sabbagh, Dan. "Boris Johnson Forced to Reduce Huawei's Role in UK's 5G Networks." *The Guardian (UK)*, May 22, 2020. Accessed June 8, 2020. Retrieved from: http://web.archive.org/web/20200617011641/https://www.theguardian.com/technology/2020/may/22/boris-johnson-forced-to-reduce-huaweis-role-in-uks-5g-networks.

way in 5G'.[43] As it stands, the question remains open as to how various governments will choose to proceed - and how they will choose to govern the direction of 5G deployment and maintenance, both nationally, and through the establishment of international norms and standards. Attempts to map changes in national policy towards 5G reveal a range of different approaches over time and between allied states[44], highlighting disparate, differing attitudes to potential governance mechanisms.

2.3 Huawei and 5G - mitigating geopolitical risk

How does a state mitigate the strategic risks of a foreign state leveraging 5G infrastructure to conduct espionage against a target state's citizens? NATO CCDCOE's 5G report highlights the inadequacy of international law to outlaw international espionage and does not recommend international law as the primary mechanism for cyber risk management.[45] The report instead argues that deployment of 5G *must* consider wider strategic geopolitical considerations in addition to technical security concerns.

The concerns around Huawei's involvement in supplying critical 5G infrastructure have been recognised around the world, but the counter-challenge to a proposed boycott highlights a shortage of appropriate alternative providers. When it comes to actors with the research and deployment capability to deploy 5G technology in a way that offers security against device compromise - *satisfying initial security concerns* - it is not necessarily the quality of the work that is being challenged; it is the wider context of supplier independence, integrity and intentions.

2.4 Transparency in the supply chain

Transparency, and a perceived lack thereof shown by Huawei and the Chinese state relating to 5G innovation, has been cited as a barrier to international partnerships. 'The fundamental question is one of trust', according to the NATO CCDCOE report[46], and this trust is challenged by perceived opaqueness and secrecy from actors across the supply chain. Potential governance mechanisms must consider these geopolitical concerns based on surveillance

---

[43] Murphy, David. "Huawei Outlines Commitment to UK's Telecoms Infrastructure with Open Letter Ads." *Mobile Marketing Magazine*, June 08, 2020. Accessed June 16, 2020. Retrieved from: https://web.archive.org/web/20200620015025/https://mobilemarketingmagazine.com/huawei-outlines-commitment-to-uk-telecoms-infrastructure-with-open-letter-ads

[44] Arumugam, Ganesan. "Huawei Ban Timeline: US Companies Allowed to Work with Huawei on 5G Standards." June 17, 2020. Retrieved from http://web.archive.org/web/20200617214401/https://www.tipsclear.com/huawei-ban-timeline-us-companies-allowed-to-work-with-huawei-on-5g-standards/.

[45] Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik. "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)* 28 (2019).

[46] Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik. "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)* 28 (2019).

capabilities and expectations of potential adversarial behaviour, and monitor technical implementation and oversight plans accordingly.

2.3 Huawei's collaboration, code-sharing, and the relative posture of competitors

To quote Huawei's chief security officer, the company is 'probably the most poked and prodded organisation' in the world.[47] For all the controversy surrounding Huawei's participation, it is important to acknowledge that Huawei has gone to great lengths to display their transparency and security credentials. With the launch of the' Cyber Security Transparency Centre in Brussels in early 2019, Huawei called on industry and governments 'to establish unified, objective cyber security standards', creating a collaborative space to develop such standards and verification mechanisms.[48] At the Centre, wireless and internet companies are able to test the networking equipment and have access to Huawei's source code, allowing potential customers the chance to verify Huawei's security infrastructures. Huawei's choice to release development code for wider scrutiny arguably makes it more transparent compared to its competitors; neither Ericsson nor Nokia offer the same access to their technology. Huawei also arguably attracts disproportionate attention due to its technical superiority, or dominance, of the 5G innovation landscape. NATO CCDCOE highlights several other Chinese technology manufacturers that are restricted from providing core infrastructure for US government networks, while noting that Huawei's technology have revealed robust security structures, with no major cyber security vulnerabilities identified.[49] Huawei offering their code for review has attracted some criticism of their security posture (including from oversight assessments from the UK's National Cyber Security Centre[50]) it is due to Huawei's transparency that such critiques are possible.

In mid-June 2020, the US Department of Commerce announced that US companies are to be permitted to develop 5G standards in collaboration with Huawei.[51] Given the US government's concerns about Huawei's role in the 5G landscape, this development highlights the complexities (and shifting priorities) in supply chain innovation. Ultimately, Huawei is one of a number of potential supply chain actors, and the US' willingness to involve Huawei in standards-setting

---

[47] Cellan-Jones, Rory. "Huawei Risk Can Be Managed, Say UK Cyber-Security Chiefs." *BBC*, 15 Feb. 2020, web.archive.org/web/20200623224017/https://www.bbc.com/news/business-47274643.

[48] Adamowicz, Jakub. "Huawei Cyber Security Transparency Centre Opens in Brussels." Huawei (EU), 5 Mar. 2019, web.archive.org/web/20200623193703/huawei.eu/press-release/huawei-cyber-security-transparency-centre-opens-brussels.

[49] Kaska, Kadri, Henrik Beckvard, and Tomáš Minárik. "Huawei, 5G and China as a security threat." *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)* 28 (2019).

[50] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, 'Annual Report', April 2019, http://web.archive.org/web/20200623230228/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[51] "Commerce Clears Way for U.S. Companies to More Fully Engage in Tech Standards-Development Bodies." *Commerce.gov*, US Department of Commerce, 15 June 2020, web.archive.org/web/20200622071118/www.commerce.gov/news/press-releases/2020/06/commerce-clears-way-us-companies-more-fully-engage-tech-standards.

highlights the integral importance of inclusive governance. It may also be an acknowledgement of changing attitudes to Huawei's involvement, or at least, Huawei's reliability relative to other supply chain actors. Time will tell whether Huawei has been a victim of broader geopolitical clashes.

III. Multistakeholder governance for 5G implementation

As noted above, several of the challenges associated with 5G implementation are technical, yet administrative and geopolitical hurdles can pose significant challenges to deployment. The implementation and management of 5G networks depend on the organisation and standardisation of technical infrastructure on a case by case basis. Different participating actors have to join together so that the whole process functions harmoniously. This means that different suppliers and managers of equipment - and software - will take part in the end-to-end 5G deployment and monitoring lifecycle. From the start, the process faces challenges only as a matter of coordination and compatibility arrangements but also in terms of security (and privacy) standards and resilience levels.

The focus of developers of Information and Communication Technologies (ICTs) tends to be efficiency in the flow of information and communication (making performance faster, more straightforward to use, reducing latency, etc). Thus, privacy and security considerations - from the ground up (by design) - tend not to receive the same emphasis world-wide. Different countries and industries do require and deploy different levels of security (and privacy).[52] As a matter of implementing this vast and complex new technology, there should be a mechanism that both provides guidance and is equipped to continuously monitor and respond to security (and privacy) issues.

The centrality of 5G in the economy across interrelated layers of industry and society makes its security risks inherently more pervasive compared with previous 2G, 3G and 4G network iterations. Take the example of self-driving cars or traffic controls. Any breakdown in communication or tampering with would have an impact beyond information breaches. [53]

3.1 Governance and risks

The risks have not necessarily changed in nature but have grown in both numbers - likely billions of new devices should be connected with 5G - and depth - it is more likely that they will have impacts on an individual's user integrity. Systemic threats to entire industries and critical

---

[52] One important level of security relates to supply chain security, differing levels of security and privacy by design deployed coupled with different levels of country orientations and regulations make it a topic of relevance. More on that see: Świątkowska, J. Supply Chain Security Beyond 5G. *In.:* directions blog, 9 April, 2020. Retrieved from: /web/20200622113116/https://directionsblog.eu/supply-chain-security-beyond-5g/.

[53] The example of self-driving cars was taken from the IDB study. 5G: The Driver for the Next-Generation Digital Society in Latin America and the Caribbean, March, 2020. Retrieved from: https://publications.iadb.org/en/5g-driver-next-generation-digital-society-latin-america-and-caribbean.

infrastructures are important elements that should be taken into account. The reliance on connected devices will most likely raise the stakes for network stability.

Another layer of risks and challenges relates to the potential connectivity and 'digital gap' that 5G will raise if not properly managed. This may happen in terms of people that may not have the resources to access the network and in terms of regions, places and territory that may not be connected. These factors highlight how technology will require greater resources than the previous iterations, hence making it likely that priority will be given to the most affluent parts of countries and cities, leaving other regions and local populations behind.

This article assumes the following threat model is applicable, with challenges including:

(i) deliberate and malicious actions against the network or targeted sectors and devices

(ii) system design flaws that may create incentives that lead to negative impacts

(iii) benevolent implementation that may have unintended perverse consequences

(iv) lack in consideration of the social, economical and cultural diversity within countries that may leave areas and people outside the network - i.e. non-inclusive or discriminatory policies.

Coupled with that is a geopolitical matter of how to better organise a reliable system that works as a global mechanism - the internet was created to be global - but respects as well an important level of national self-determination - i.e. sovereignty.[54] The Internet was organized to be distributed and decentralised, which did not prevent power imbalances relative both to countries and companies.[55] This leaves a potential security risk, particularly related to a worldwide supply chain that involves countries and companies with different views on how the network should work, be managed and which values it should foster.

3.2. Models for 5G governance: appropriate ways forward

[54] Timmers, P. There will be no global 6G unless we resolve sovereignty concerns in 5G governance. *In.: Nat Electron* 3, 10–12 (2020). Retrieved from: https://doi.org/10.1038/s41928-020-0366-3. See as well: Kieron O'Hara and Wendy Hall. Four Internets: The Geopolitics of Digital Governance. CIGI Papers No. 206 — December 2018. Retrieved from: /web/20200622113405/https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf.

[55] Timmers, P. The Geopolitics of standardization. *In.:* directions blog, 9 April, 2020. Retrieved from: /web/20200622113613/https://directionsblog.eu/the-geopolitics-of-standardisation/.

Behind and parallel to these security (and privacy) questions is a major variable that may influence each aspect highlighted above: the governance regime that better implements and manages 5G technologies.[56]

As O'Hara has already pointed out for the digital environment as a whole, "[e]very design decision reflects, and imposes (perhaps unconsciously), a balance of power, while cultural, economic and political tensions play out across the collective-action problems generated by digital modernity."[57] Thus, an emphasis on the decision making process, from planning to deploying and even maintaining 5G technology, should be at the forefront of any governance arrangement.

This means there are key decisions that should be taken to safeguard the security of the 5G network. This comes under at least two levels, a governance arrangement and its connection to a geopolitical approach.[58] For the latter, there are four options from the standpoint of governments that should be taken into account: (1) an isolationist model, based on independence and autonomy; (2) a partnership model based on a like-minded, like-value group of trusted countries; (3) an opened model based on shared standards and an agreed minimum consensus on security and privacy levels; and (4) a hybrid model which is opened in certain aspects and closed in others, a risk management approach.[59]

---

[56]There are many different definitions of governance. In this paper, the term refers to a structure: the architecture of the institutions in charge of decision-making, and the steering processes for achieving the implementation and management of 5G. For more on different options of conceptualizing governance, see: Levi-Faur, D. The Oxford Handbook of Governance. OUP, 2012.

[57] O'Hara, K. and Hall, W. Four Internets: The geopolitics of Digital Governance. *In.:* CIGI, Dec. 2018. Retrieved from: /web/20200622113405/https://www.cigionline.org/sites/default/files/documents/Paper%20no.206web.pdf.

[58] When thinking of internet governance as a whole, the standpoint tends to always depart from the global aspect of the network. Yet, from the deployment of a infrastructural technology there seems to be more of an interaction between a national deployment of technology and an international arrangement that it will part-take. Solum analysing from the view of internet governance parts from a global approach. See for that: Solum. L. Models of Internet Governance. *In.:* Bygrave, L. A. and Bing, J. Internet Governance: Infrastructure and Institutions. OUP, 2009. Further on that: Hoxtell. W. and Nonhoff, D. Internet Governance: Past, Present and Future. KAS, 2019. Retrieved from: http://web.archive.org/web/20200622003058/https://www.gppi.net/media/Internet-Governance-Past-Present-and-Future.pdf; Niesyto, J., Otto, P. Who governs the internet? Players and fields of action. Friedrich-Ebert-Stiftung, 2017. Retrieved from: http://web.archive.org/web/20200622003005/http://library.fes.de/pdf-files/akademie/13910.pdf.

[59] The models described here have been conceptualized taking into consideration the approaches to strategic autonomy suggested by Timmers. More on that: Timmers, P. here will be no global 6G unless we resolve sovereignty concerns in 5G governance. *In.: Nat Electron* 3, 10–12 (2020). Retrieved from: http://web.archive.org/save/https://www.nature.com/articles/s41928-020-0366-3. See also: EU Cyber Direct - Policy in Focus: Strategic Autonomy and Cybersecurity. Retrieved from: http://web.archive.org/web/20200622002240/https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf.

As for the governance arrangement,[60] the institutional structure may take different formats. Industry actors might be left to follow their discretion, and be considered responsible (and liable) for any security breaches.[61] There could be a central focal public institution that may coordinate 5G deployment. Governments may do more than coordinate, and may take the active role of driving standards-setting and deployment practices. There can be a partnership between governments and industry. Finally, there can be an arrangement that is more open and allows for the participation of different stakeholders, whether under an independent institution, a governmental agency or a department from the administration.

3.3 The advantages of multistakeholder governance arrangement:

Some actors tend to advocate in a certain direction more than others. The significant resources needed in terms of investment, as well as the necessary technical expertise to deploy and manage 5G networks, both imply the need for active participation from the private sector.[62] Equally relevant is the fact that both governments and the economy as a whole have become centrally dependent on internet connectivity. With the deployment of 5G, internet dependence will only increase as more devices are connected to the online network (IoT - smart cities, smart industries, smart farms). The result is that it becomes a complex, yet centrally important, affair to organise, understand and manage such networks. Some countries have been vocal that it is a matter of sovereignty.[63] Hence, governments have a legitimate claim to be involved.

In many cases, the interaction between private and public sectors is what either generates governance, or results in a dialogical process that will in itself serve as a governance mechanism.[64] In several countries, particularly in the global south, neither companies nor the administration will be able to alone bear the burden of implementing and managing 5G technologies. The needs of both sectors will intertwine commanding a governance regime that involves them both.

Additionally, society as a whole is and will continue to be affected by the decisions related to the standards of security (and privacy) for 5G technology, not to mention the impact on individual rights. The complexity of network security concerns, alongside the several dimensions of implications introduced above, supports the idea that all sectors with a stake in the matter

---

[60] To some extent *mutatis mutandi* the logic applies to international arrangements as well.

[61] The case of Australia seems to fit this logic.

[62] Rosemberg, D. How 5G will change the world. World Economic Forum, 2018. Retrieved from: /web/20200622113744/https://www.weforum.org/agenda/2018/01/the-world-is-about-to-become-even-more-interconnected-here-s-how/.

[63] One example is France's President. Emmanuel Macron, which considered that choices regarding the development, standardization and implementation of 5G were involved sovereign decisions that should not be fully left for the private sector to decide. See: Macron and the future of Europe. *In.: The Economist,* (9 November 2019).

[64] World Economic Forum, White Paper. Global Technology Governance: A Multistakeholder Approach, October 2019. Retrieved from: /web/20200622113840/http://www3.weforum.org/docs/WEF_Global_Technology_Governance.pdf.

should have a seat at the table. The technical sector, academia and civil society can and should contribute to its governance.[65] Their different perspectives brought together tend to strengthen the governance architecture and offer more legitimacy to both the structure and the process it does and will foster. In short, a multistakeholder governance arrangement seems to fit the bill.[66]

The fact that 5G will become a key facilitator for internet connectivity makes it relevant that its governance arrangement aligns with wider internet governance infrastructure. Comprehensive governance infrastructure reinforces 5G governance capabilities. In the case of the internet, its complexity and design are motivating forces for inclusive participation. Some argue that the existing approach to internet governance is inherently multistakeholder, as all attempts to steer from one standpoint alone will find push backs from other actors.[67] As 5G becomes embedded as a structural feature of online technology, many of the features that make a multistakeholder model of governance a good fit for internet governance are shown to be appropriate for an extension to 5G security management.

IV. A Case Study in Multistakeholder Governance - The Brazilian Internet Steering Committee (CGI.br)

Several multistakeholder internet governance models have been experimented both in the international and the national levels and may serve as templates for 5G security governance.

---

[65] On governing the internet as a whole, this has been argued many times in a similar way. One view can be found at: Souter, D. Inside the Information Society: Multistakeholder participation, a work in progress. *APC (blog)*, (February, 2017). Retrieved from: /web/20200622113920/https://www.apc.org/en/blog/inside-information-society-multistakeholder-participation-work-progress.

[66] From the standpoint of international scholarship, multistakeholderism relates to a form of governance that is more inclusive and aggregates or allows participation of different stakeholders. See: Raymond, M. and Denardis, L. Multistakeholderism: anatomy of an inchoate global institution. International Theory, May 2015. Retrieved from: https://doi.org/10.1017/S1752971915000081.

[67] Esterhuysen, A. Global Mechanisms to Support National and Regional Multistakeholderism. *In.:* Drake, W.J. & Price, M. (Eds.) Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem. 2014. Retrieved from:/web/20200622114414/https://global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf. See as well: Cerf, V. Internet governance: A centroid of multistakeholder interests. *In:* M*ultistakeholder Internet Dialogue (MIND)* (2011), Internet Policy Making - Collaboratory Discussion Paper Series No.1, vol. 2.

This paper will examine as a case study the Brazilian Internet Steering Committee (CGI.br) for properly responding to the challenges of multistakeholder governance.[68]

4.1. Configuring multistakeholder governance - CGI.br:

The Brazilian Internet Steering Committee (CGI.br) was created in 1995 by the Ministries of Science and Technology (and Ministry of Communications) - through Interministerial Ordinance 147 of May 31st, 1995 - to serve as an advisory board for Internet matters. It was *ab initio* a plural entity involving different stakeholders connected to the internet - such as the government, business, non-profit and non-commercial entities, academia and the scientific and technological community.[69] The multistakeholder nature has increased over time and the following features foster and guarantee the continuation of such aspects.

Composition

In 2003, during President Lula's mandate, the Committee was reformed[70] and civil society gained more space. The Committee currently has 21 representatives. These include 9 from governmental agencies and 12 from civil society - including academia, technicians, civil society organizations, and the private sector.[71] Thus, the overall composition responds to the needs of government while also allowing for civil society at large to contribute to the discussion, and hold the capacity to be heard.

Selection process

---

[68] This paper is not alone in analyzing the CGI.br as a potential template for multistakeholder governance. See, for instance: UNESCO, What if we all governed the internet. 2016. Retrieved from: https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf; Canineu, M. L. and Donahoe, E. Brazil as the Global Guardian of Internet Freedom? In.: Amnesty International Netherlands, 2014. Retrieved from: /web/20200622114454/https://www.amnesty.nl/content/uploads/2014/11/rising_power_brazil.pdf. For a parallel view of different internet governance arrangements see: Drake, W. (org.). *The Working Group on Internet Governance - 10th anniversary reflection*s. 2015. Retrieved from: /web/20200622114526/https://www.apc.org/sites/default/files/IG_10_Final.pdf; and for a recent exploration see: Belli, L; Canabarro, D.; Herzog, J.; Hill, R.; Souza, C. A.; and Trumpy, S. Explorando a governança multissetorial na Internet: rumo à identificação de um modelo de órgão consultivo de políticas da Internet [*Exploring multistakeholder internet governance: charting a path to identifying a model for a consulting body to settle internet policy*]. April, 2020. Retrieved from: /web/20200622114619/https://politics.org.br/edicoes/explorando-governan%C3%A7a-multissetorial-na-internet-rumo-%C3%A0-identifica%C3%A7%C3%A3o-de-um-modelo-de-%C3%B3rg%C3%A3o.

[69] Further information available at: /web/20200622114720/https://cgi.br/about/.

[70] Brazilian Presidential Decree 4,829 of September 3rd, 2003.

[71] Canabarro, D. R.; Borne, T. The Brazilian Reactions to the Snowden Affairs: implications for the study of International Relation in an Interconnected World. Session: The Incorporation of processes and agendas of international politics in Brazil. *In.:* Conjuntura Austral, Porto Alegre, v.6, n.30, jun. / jul. 2015 2015. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155476.

One of the main criticisms of different multistakeholder governance structures is the opacity of the appointing or selection mechanism.[72] The CGI, however, follows a different path. Until 2002, even if under a plural basis, the members were appointed by the Federal Government. Under the 2003 reform, representatives are elected through an open and transparent process, where entities that are a part of the internet environment enlist to participate in the election.[73]

Normative and agenda-setting efforts

According to the Presidential Decree 4,829, the CGI has the following attributions: (i) to propose policies and procedures related to the regulation of Internet activities; (ii) to recommend standards for technical and operational procedures; (iii) to promote studies and recommend technical standards for the network and services' security in the country.[74] As may be noticed, the decisions do not usually have a binding nature. CGI intends to foster a collaborative atmosphere, where the internet ecosystem is a willing participant and very much inclined to adhere to the recommendations of the steering committee. Similar aspects may help foster a collaborative environment to deal with 5G security issues.

The decision-making process

The logic of the Committee is to facilitate a broad-based dialogue, bringing parties together to increase both representativity and legitimacy.[75] All members have equal footing in the decision-making process. This is highlighted by its consensus-based arrangement.[76] Traditionally decisions are only achieved when all members of the CGI are satisfied therewith. In the both competitive and geopolitically complex environment of 5G governance, a consensus and broad base arrangement may be challenging but also may provide the best long term results.

Autonomy

Besides having administrative and technical autonomy, the funding system enhances its financial independence. The Committee sources revenue through the fees collected by NIC.br -

---

[72] More on such types of criticisms under internet governance, see: UNESCO, What if we all governed the internet. 2016. Retrieved from: https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf.

[73] More on the election process: /web/20200622114859/https://www.cgi.br/processo-eleitoral/.

[74] Further specifications of the attributions of the CGI.br, see: /web/20200622114820/https://www.cgi.br/atribuicoes/.

[75] Lemos, R.; Souza, C. A.; Steibel, F.; and Nolasco, J. Fighting Spam the Multistakeholder Way – A Case Study on the Port 25/TCP Management in the Brazilian Internet, 2015. Retrieved from:http://ow.ly/O3jVQ.

[76] Glaser, H. e Canabarro, D. "Before and after the WGIG: Twenty years of multistakeholder Internet governance in Brazil" em Drake, W. (org.). *The Working Group on Internet Governance - 10th anniversary reflections*. 2015. Retrieved from: http://web.archive.org/web/20200214154705/https://www.apc.org/sites/default/files/IG_10_Final.pdf .

the private non-profit organization in charge of administering the ".br" in the domain name system.[77] This tends to guarantee that the decisions of the regime will not be constrained by governmental funding or private resources.

Normative pillar

Another feature of the Steering Committee is that it has developed a normative principle-based approach for the governance and use of the internet. It is referred to as the "Decalogue".[78] It is a normative embodiment of certain basic values and principles:

(1) freedom, privacy and human rights;

(2) democratic and collaborative governance

(3) universality

(4) diversity

(5) innovation

(6) network neutrality

(7) non-liability of network intermediaries for actions performed by end-users

(8) functionality, security and stability

(9) standardisation and interoperability

(10) proper legal and regulatory environments

This categorisation functions as guidance for the overall governance arrangement and almost a 'constitutional' basis, expression of fundamental values and a consensus among the different stakeholders. As for 5G, a similar set of principles should be sought to apply. It may provide a stable basis for the whole governance framework.

4.2 The Brazilian Internet Steering Committee (CGI.br) as a model for 5G governance

The Brazilian Internet Steering Committee as discussed above provides an important framework for discussing 5G governance. Its features solve or facilitate an important part of the challenges 5G technology will bring. As noted above, security and privacy challenges are rooted in different views on how to standardize deployment and management of the technology coupled with a lack of overall trust and a geopolitical complex context.

---

[77] Further info:http://web.archive.org/web/20200622105157/https://nic.br/.

[78] Canabarro, D. R.; Borne, T. The Brazilian Reactions to the Snowden Affairs: implications for the study of International Relation in an Interconnected World. Session: The Incorporation of processes and agendas of international politics in Brazil. In.: Conjuntura Austral, Porto Alegre, v.6, n.30, jun. / jul. 2015 2015. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155476.

Trust and confidence amongst the stakeholders is paramount to tackle such challenges. Open participation with elected representatives creates an environment that invites transparency and provides the necessary checks and balances to achieve sound policy. The fact that decisions are based on consensus and may be anchored on a set of pre-arranged principles make it easier for acceptable actions to flow from ample dialogue. The involvement of civil society provides as well outlets for the community as a whole to be informed and take part. It also serves as a guarantee that decisions will not be taken in closed doors with the sole aim of benefiting a few. Academia also serves in part this role but it goes further providing potentially a technical and theoretical framework. Such characteristics will be important in any governance arrangement for 5G.

Conclusion

The opportunities of 5G technology are transformative due to the enhanced connectivity (and interconnectivity) of IoT communications, and telecommunications are one domain in which this has immediate deployment opportunities. Significant technical, administrative and geopolitical challenges require the attention and overview of an inclusive and sound governance framework, to best ensure 5G technology is deployed and managed in as secure a methods as possible, including in privacy terms.

As the Huawei and 5G case study has shown, there is currently no consensus on best-practice governance models. The security risks coupled with the political complexities make it a challenge to design the best governance infrastructure for 5G. This paper shows that it is also an opportunity. Inclusive governance arrangements that can bring all stakeholders to the table and facilitate a dialogue, are capable of generating trust and a stable environment for 5G deployment and management.

By outlining the structures and advantages achieved through multistakeholder governance - as currently applied through internet governance mechanisms - this article proposes that 5G could benefit from an extension of a similar approach. The model utilised for the Brazilian Internet Steering Committee (CGI.br) seems to provide some of the features that are necessary for an institutional implementation of a functioning multistakeholder 5G governance structure. It may serve as a potential template for developing similar arrangements for the governance of 5G technology.