Conceptualizations of 5G

POL61305: Emerging Technologies and International Security

Author redacted

May 22, 2020

5G is the next generation of mobile telecommunications technology. It represents a step change in what is possible with wireless networks, and will lead to a vastly increased number of use-cases that are embedded more deeply into the fabric of society than is currently the case. Potential uses include smart cities, self-driving cars, and internet of things devices.

While this has the potential to unlock huge economic growth, it also makes mobile networks a critical dependency of a modern economy and as such, control over the development and implementation of 5G technology has been heavily securitized.

This paper constitutes a narrative literature review of the security aspects of 5G, and as such, aims to outline the different views, approaches, theories and models used by various scholars and real-world actors. This includes a description of different models of technological development that are used to conceptualize 5G, realist and neoliberal views of how 5G affects the world order, and finally, a description of conspiracy theories around 5G.

1 Introduction

5G is the fifth and latest generation of mobile phone technology, which is currently being deployed worldwide. Unlike previous generations of mobile phone technology, 5G adoption has been heavily securitized [1] and controversial.

In the review, relevant papers were identified by searching Google Scholar using the terms "5G", "international security", "national security", and by searching for literature among prominent think tanks and international organizations such as Chatham House, United Nations Institute for Disarmament Research (UNDIR), Center for New American Security (CNAS), Center for Strategic and International Studies (CSIS), German Council on Foreign Relations (DGAP) etc. Citations were then followed from the above sources in order to get a comprehensive overview of the current literature on the security relevant aspects of 5G.

2 Categorical Interpretations of 5G

There are multiple competing and overlapping technological frameworks which can be used to categorize 5G, plausible selection of which is outlined. Rotolo, Hicks and Martin outline a definition for '*emerging technology*' based off of five criteria, which serve as a basis to ascertain whether a given technology such as 5G can be classed as 'emerging' [2]. More broadly, Banta describes the field of *technology assessment* [3], which is aimed at predicting the longer term outlook of a technology, and this framework is used by the US Department of Defence to better understand the potential effects of 5G [4].

Related to technology assessment, the EU has undertaken a *risk assessment* of 5G in order to better understand the differences between it and previous versions of mobile networks, and the consequent risks of 5G adoption [5]. Various think tanks in the US [6] and the EU [7], as well as UNDIR [8] having taken this approach, focusing on supply chain security in particular as summarized by US-based nonprofit MITRE [9].

A less convincing interpretation of 5G is that of a '*disruptive innovation*' as defined by Christensen [10] (though competing definitions exist, see Kawamoto and Spers [11]), or as a *military innovation* as defined by Horowitz and Pindyck [12].

3 Realist conceptualizations

Many actors consider 5G within a realist framework, where policies arise from the unregulated competition between states [13] and interactions between states are regarded as zero sum. The German think tank SWP sees 5G as a contested technological sphere of influence that is part of a larger rivalry between the US and China [14; 15; 16] with Europe in the middle and without a strong foreign policy stance of its own (though able to wield regulatory power to exert some measure of influence [17]). Another German think tank, DGAP highlights China's use of strategic subsidies to advantage Huawei at the expense of European suppliers and (indirectly) Germany's national security and democratic values [18]. The NATO Cooperative Cyber Defence Center of Excellence recently released a paper to the same effect [19], raising the point that there is precedent for China to exploit its technological advantages for SIGINT operations [20], and describing the opaque ownership structure of Huawei, which suggests covert state involvement [21; 22].

China certainly sees itself as playing an adversarial role in a realist world; the US has repeatedly leveled the charge of high-tech intellectual property theft against China [23; 4; 24; 25]. Such a viewpoint sees the many geopolitical advantages gained from dominance over 5G, especially since as many emerging technology scholars have pointed out new threats caused by new technologies such as 5G can develop over time [26; 27].

Some realist viewpoints, prominently advocated for by the US, argue for preventing Chinese infiltration of 5G networks by banning Huawei equipment altogether [4]. However, risk consultancy Eurasia Group warn that barring Huawei could have serious effects on the market structure for 5G, especially if international cooperation is degraded and incompatible standards emerge [28]. Furthermore, Lysne outlines the need for 'heterogeneity of suppliers' as critical part of an effective approach for 5G security, which would be far harder with a highly segmented market [29].

4 Neoliberal conceptualizations

Neoliberalism aims to build coordination and cooperation among nation states through international organizations, and takes a more constructive view of how states can interact [30].

Like the US, the UK acknowledges the threats that China poses in the 5G supply chain [31], but has responded by working with China to set up a review board with access to Huawei software and hardware that aims to review it for exploitable threats [32] (in line with what the think tank SNV suggests [33]). Chatham House points out that the UK's existing mobile network infrastructure has a strong path dependence on 5G [34], which goes towards explaining this engaged and somewhat mitigatory approach.

The EU takes a typically non-aggressive and neoliberal approach. It doesn't reject Huawei but instead gives member states cover to do it of their own accord through its critical 5G Cybersecurity report [35]. That said, the EU's cybersecurity agency notes that supply chain attacks are only one vector by which 5G could be used for malicious purposes, viewing Huawei's trustworthiness as an issue less important to the overall picture of 5G security, but sees 5G as an important and complex threat overall [36].

The EU is built on the idea that trade helps to reduce conflict, yet scholars such as Henry Farrell are moving back towards a realist view by showing how trade can be weaponized to undermine this foundation, and how Huawei is an example of China has failing to integrate properly into the global neoliberal economic system [37]. A recent paper from the Carneige Endowment for International Peace describes how the EU is shifting to a more aggressive approach in order to maintain it's multilateral approach in this more adversarial environment [38].

Going forward the German think tanks SWP and SNV suggest the EU could try other multilateral solutions than trade, such as trying to export its cybersecurity laws to other places in order to bolster the security and resilience of the whole ecosystem [17; 39].

5 Misconceptions of 5G

Recent empirical observations have shown members of the general public to be intensely skeptical of 5G, with multiple studies describing misinformation campaigns and conspiracy theories that associate 5G as a causative factor for the 2020 coronavirus pandemic [40; 41; 42]. This has had a particular impact in the UK, where mobile network base stations have been destroyed [40] and the National Government has issued advice to citizens that there is no link between the 2020 coronavirus pandemic and 5G [43]. Yet the scientific consensus does not pervade all of Government, Glastonbury Town Council recently released a controversial report by it's 5G Advisory Committee on the dangers and risks of 5G to human health [44].

6 Conclusions

In line with the Collingridge dilemma [45], the effects of 5G on society will only be revealed as it is implemented. In the midst of this uncertainty, this paper has examined the literature on 5G from a range of actors, examining how 5G is conceptualized and the real world effects it is having on the behaviour of actors on the world stage.

For nation states, trustworthiness of suppliers is of vital importance since 5G technology is hard to verify. As such, further research on the relationship between the market structure of 5G and the trustworthiness of vendors is important and required in order to explore how states can use collaborative and economic tools such has competition law to improve the overall health of the 5G ecosystem.

Similarly, more research is warranted on how 5G is framed by actors and perceived by ordinary users. While conventional wisdom may consider 5G as a public technology which contributes to the public good (as defined by Drezner [23]), the wealth of misinformation around 5G suggests that it has potential to be understood differently. This is important, since different disinformation campaigns targeting 5G and other emerging technologies could be used as a hybrid warfare tactic by malign actors [46] in future conflicts.

References

[1] Thierry Balzacq, Sarah Léonard, and Jan Ruzicka. 'securitization'revisited: Theory and cases. *International Relations*, 30(4):494–531, 2016.

[2] Daniele Rotolo, Diana Hicks, and Ben R Martin. What is an emerging technology? *Research policy*, 44(10):1827–1843, 2015.

[3] David Banta. What is technology assessment? *International journal of technology assessment in health care*, 25(S1):7–9, 2009.

[4] Center for Strategic and International Studies (CSIS). CSIS panel on Emerging Technologies Governance, 2020.

[5] NIS Cooperation Group. Eu coordinated risk assessment of the cybersecurity of 5g networks. 2019.

[6] Center for Strategic and International Studies (CSIS). Twin pillars: Upholding national security and national innovation in emerging technologies governance. 2020.

[7] Jan-Peter Kleinhans. Whom to trust in a 5g world? policy recommendations for europe's 5g challenge. 2019.

[8] UNDIR. Stemming the exploitation of ict threats and vulnerabilities. 2019.

[9] Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof. *Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war*. MITRE Corporation, 2018.

[10] Clayton M Christensen, Michael E Raynor, and Rory McDonald. What is disruptive innovation. *Harvard business review*, 93(12):44–53, 2015.

[11] Carlos Tadao Kawamoto and Renata Giovinazzo Spers. A systematic review of the debate and the researchers of disruptive innovation. *Journal of technology management & innovation*, 14(1):73–82, 2019.

[12] Michael C Horowitz and Shira Pindyck. What is a military innovation? a proposed framework. *A Proposed Framework (December 15, 2019)*, 2019.

[13] Jack Donnelly. *Realism and international relations*. Cambridge University Press, 2000.

[14] Peter Rudolf. The sino-american world conflict. 2020.

[15] Barbara Lippert and Perthes Volker. The sino-american world conflict. 2020.

[16] Barbara Lippert and Perthes Volker. Strategic rivalry between united states and china. 2020.

[17] Annegret Bendiek and Martin Schallbruch. Europe's third way in cyberspace: what part does the new eu cybersecurity act play? 2019.

[18] Kaan Sahin and Didi Tatlow. Berlin's preliminary 5g decision. 2019.

[19] Kadri Kaska, Henrik Beckvard, and Tomas Minarik. Huawei, 5g and china as a security threat. *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)*, 28, 2019.

[20] Chris C Demchak and Yuval Shavitt. China's maxim–leave no access point unexploited: The hidden story of china telecom's bgp hijacking. *Military Cyber Affairs*, 3(1):7, 2018.

[21] Colin Hawes and LI Grace. Transparency and opaqueness in the chinese ict sector: A critique of chinese and international corporate governance norms. *Asian journal of comparative law*, 12(1):41–80, 2017.

[22] Stacie Hoffmann, Samantha Bradshaw, and Emily Taylor. Networks and geopolitics: How great power rivalries infected 5g. *Oxford Information Labs, August*, 22:4, 2019.

[23] Daniel W Drezner. Technological change and international relations. *International Relations*, 33(2):286–303, 2019.

[24] Center for Strategic and International Studies (CSIS). Tech-politik: Historical perspectives on innovation, technology, and strategic competition. 2019.

[25] United States. Office of the US Trade Representative. *Findings of the Investigation Into China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*. Office of the United States Trade Representative, Executive Office of the . . . , 2018.

[26] Aharon Hauptman. Illuminating the "dark side" of emerging technologies. In *Emerging technologies for economic development*, pages 263–285. Springer, 2019.

[27] Tadas Limba, Andrius Stankevičius, and Antanas Andrulevičius. Industry 4.0 and national security: the phenomenon of disruptive technology. 2019.

[28] Paul Triolo and Kevin Allison. The geopolitics of 5g. *Eurasia Group White Paper, Nov*, 15:1811–14, 2018.

[29] Olav Lysne. *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment?*, volume 4. Springer, 2018.

[30] Robert Owen Keohane. *Neorealism and its Critics*. Columbia University Press, 1986.

[31] Media & Sport UK Government Department for Digital, Culture. Uk telecoms supply chain review report. 2018.

[32] UK Cabinet Office, National Security, and Intelligence. Huawei cyber security evaluation centre oversight board: annual report 2019. 2019.

[33] Jan-Peter Kleinhans. 5g vs national security: a european perspective. *Stiftung Neue Verantwortung, Feb*, 2019.

[34] Emily Taylor. Who's afraid of huawei? understanding the 5g security concerns. 2019.

[35] EU Commission. Cybersecurity of 5g networks. 2019.

[36] ENISA (European Union Agency for Cybersecurity). Enisa threat landscape for 5g networks. 2019.

[37] Henry Farrell and Abraham Newman. Weaponized globalization: Huawei and the emerging battle over 5g networks. *Global Asia*, 14(3):8–12, 2019.

[38] Erik Brattberg and Philippe Le Corre. The eu and china in 2020: More competition ahead. 2020.

[39] Kate Saslow. Global cyber resilience: thematic and sectoral approaches. 2019.

[40] Wasim Ahmed, Josep Vidal-Alaball, Joseph Downing, and Francesc Lopez Seguí. Dangerous messages or satire? analysing the conspiracy theory linking 5g to covid-19 through social network analysis. *J. Med Internet Res*, 2020.

[41] Shadi Shahsavari, Pavan Holur, Timothy R Tangherlini, and Vwani Roychowdhury. Conspiracy in the time of corona: Automatic detection of covid-19 conspiracy theories in social media and the news. *arXiv preprint arXiv:2004.13783*, 2020.

[42] Lotte Pummerer and Kai Sassenberg. Conspiracy theories in times of crisis and their societal effects: Case "corona". 2020.

[43] Department for Digital, Culture, Media & Sport. 5G and coronavirus (COVID-19), 2020.

[44] Glastonbury Town Council. Report and Recommendations from Glastonbury Town Council's 5G Advisory Committee, 2020.

[45] David Collingridge. The social control of technology. 1982.

[46] Frank Bekkers, Rick Meessen, and Deborah Lassche. *Hybrid conflicts: the new normal?* Den Haag: TNO, 2019.