Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

5G Regulation and Geopolitical Tensions

Article History:

Name of Author:
Ashley Robbins[1], Karen Neal[2], Jacqueline Gilbert[3], Troy Harris[4] and Brandon Nguyen PhD[5]

Affiliation: [1]Associate Professor, Department of Business Analytics, Balkan University of Technology, Serbia
[2]Head of Department, School of Business, Danube International University, Austria
[3]Associate Professor, Department of Banking and Insurance, Kyoto Central University, Japan
[4]Research Associate, School of Economics and Commerce, Danube International University, Austria
[5]Senior Research Fellow, Department of Banking and Insurance, Pacific Coast University, Chile
Corresponding Author: Ashley Robbins

How to cite this article: Ashley Robbins, *et, al.* 5G Regulation and Geopolitical Tensions. *J Community Med* 2020;(1);32-35.

Abstract: Fifth-generation (5G) networks represent a technological leap in speed, connectivity, and capacity—but their development has become as much a geopolitical battleground as a technical milestone. This article explores the intersection of 5G regulation and international relations, analyzing how different countries approach 5G deployment through the lenses of security, legal frameworks, and global alliances. It compares key regulatory models from the United States, European Union, China, and Asia-Pacific, highlighting diverging priorities such as innovation, privacy, and national security. Central to this analysis is the role of 5G cybersecurity mandates, vendor bans—especially targeting Chinese firms like Huawei—and spectrum allocation policies. The article also discusses the rise of techno-nationalism and the risks of a splintered global digital infrastructure. Through comparative data, case studies (such as the US Clean Network and the EU 5G Toolbox), and forward-looking insights, it evaluates how 5G regulation is shaping—and being shaped by—international power dynamics, trade policy, and the emerging blueprint for 6G.

Keywords: 5G regulation, global 5G policy, Huawei ban, Clean Network, 5G cybersecurity, EU 5G Toolbox, techno-nationalism, geopolitical tensions, spectrum auctions, data sovereignty, network security,

INTRODUCTION

The rollout of fifth-generation (5G) wireless networks heralds a new era of ultra-fast, low-latency connectivity, enabling applications from autonomous vehicles to smart cities. Yet, beyond its technical prowess, 5G technology has become inextricably linked with global policy, security, and rivalry. This research article explores how 5G regulation interfaces with mounting geopolitical tensions, focusing on divergent national legal frameworks, security concerns, and the wider implications for global trade and strategic alliances.

1. THE GLOBAL 5G REGULATORY LANDSCAPE

Core Elements of 5G Regulation

5G regulation encompasses spectrum allocation, security mandates, equipment certification, data privacy, and cross-border interoperability. All participants—telecom operators, device manufacturers, regulators, and end-users—must navigate this

intricate legal terrain for safe and effective network deployment[1][2].

International Approaches

- **United States:** Prioritizes innovation and rapid deployment, emphasizing market competition and lighter regulatory pressure. Security statutes increasingly target equipment sourced from high-risk vendors, particularly Chinese firms[3].
- **European Union:** Focuses on stringent data privacy and network security. The EU adopted the "5G Cybersecurity Toolbox" to mitigate risks, especially from non-EU suppliers, and many member states have imposed outright bans or tight restrictions on Chinese vendors like Huawei and ZTE[4][5].
- **China:** Leverages centralized investment and regulatory control to ensure rapid nationwide 5G coverage, aiming for global technological dominance.
- **Other Asia-Pacific (Japan, South Korea):** Combine high-speed rollout strategies, tailored technical standards, and public-private collaboration[3].

Region	Regulatory Priority	Example Policy/Tool
US	Innovation, national security	FCC 5G fund, Clean Network
EU	Security, privacy, supplier vetting	5G Toolbox, GDPR compliance
China	State-led rollout, self-sufficiency	5G National Plan
Japan/S. Korea	Public-private partnership, safety	Unique technical standards

2. 5G Security: The Central Regulatory Pillar

5G networks expand attack surfaces due to decentralized architecture and the proliferation of connected devices. Security frameworks thus dominate regulatory agendas:

- **Zero Trust Frameworks:** Only authenticated components may access the network, with "never trust, always verify" principles now standard in leading policies[6].
- **Cryptographic Controls:** Mandated use of hardware security modules and public key infrastructure for network authentication and data protection[7][8].
- **Vendor Assessment:** Equipment from vendors deemed "high risk" (mainly Chinese) is restricted, affecting procurement decisions, especially in EU and US markets[4][9].

3. Geopolitical Tensions Shaping 5G Regulation

US–China Rivalry

Allegations that Chinese firms (Huawei, ZTE) could facilitate state surveillance prompted the US and its allies (the "Five Eyes": US, UK, Canada, Australia, New Zealand) to ban or restrict Chinese 5G equipment on national security grounds[10][9]. The US "Clean Network" initiative institutionalized these policies, pressuring allies to follow suit.

THE EUROPEAN DILEMMA

Although the EU has taken steps to reduce reliance on Chinese tech, political and economic divisions persist. Several member states have banned Chinese vendors from 5G core networks, while others proceed with partial restrictions or compensation schemes for replacing high-risk elements[4][5]. Full de-risking is costly, and some countries remain heavily dependent on Chinese technology as rollout continues.

Other Regions

In the Middle East and parts of Africa and Latin America, Chinese 5G equipment remains prevalent due to attractive pricing and financing. These countries have sought to balance US security pressure with the economic benefits of Chinese partnerships, often leading to hybrid approaches[11].

The Rise of Techno-Nationalism

5G has become a proxy battleground for broader economic and strategic competition[12]. Control over network infrastructure is seen as pivotal for future leadership in AI, the Internet of Things, and industrial automation.

4. Key Legal and Regulatory Instruments

- **Spectrum Auctions:** National regulators, including the US FCC and counterparts in India, the UK, and the EU, allocate radio spectrum for 5G on a licensed basis, often imposing specific requirements on network security and vendor qualification.
- **Data Protection Laws:** The EU's GDPR applies to data processed on 5G networks, with implications for international data transfers and cross-border services[3].

- **5G Cybersecurity Toolkits:** Mandate technical standards, supplier risk assessments, and rapid breach notification protocols[4].
- **National Security Orders:** The US, Australia, and others have passed executive orders or legislation to restrict procurement from foreign vendors deemed national security risks[10].

5. Challenges in Harmonization and Market Access

- **Divergent Standards:** While 5G New Radio (5G-NR) is a unified global standard, national security requirements and supplier bans result in significant fragmentation[13][2].
- **Cost Implications:** Replacing high-risk vendors with "trusted" alternatives often raises costs and can delay deployment, posing challenges for nations with limited resources[5].
- **International Cooperation:** The absence of unified international 5G security standards complicates cross-border operations for network operators and global technology firms[2].
- **Compliance Complexities:** Operators must maintain separate supply chains and compliance protocols in different regions, inflating costs and operational risk.

6. Graphs and Visualizations

Global Number of Countries Banning Chinese 5G Equipment (2018–2025)

[image:1]

Graph illustrates the increase in nations imposing partial or total bans on Chinese 5G suppliers after 2018, correlating with US-led diplomatic pressure and cybersecurity incidents.

5G Network Vendor Market Share (2025 Estimate)

[image:2]

Pie chart estimating global market share of 5G infrastructure vendors, highlighting the reduced presence of Chinese firms in advanced economies but continued dominance in large emerging markets.

7. CASE STUDIES

The EU's 5G Cybersecurity Toolbox (2020–2025)

Eleven EU member states have instituted laws to block or restrict high-risk vendors in their 5G rollouts, but more than half the bloc remains dependent on Chinese equipment for parts of their networks. Only a handful of countries, like Denmark and Sweden, have completely eliminated Chinese components, often with compensation policies for mobile operators facing higher costs[4][5].

The US Clean Network Program

Banning Huawei and other Chinese companies from 5G core and non-core networks, the program has led to significant shifts in supply chains, tech alliances, and diplomatic engagement. Despite the costs, the program's proponents argue it protects critical infrastructure against espionage and sabotage[10][9].

8. Looking Ahead: 5G and the Next Generation of Geopolitics

- **Digital Sovereignty:** Nations view mastery of 5G networks as vital to sovereignty, economic competitiveness, and security.
- **Splintered Internet:** Regulatory and supply chain segregation along geopolitical lines could herald a new "splinternet"—a deeply fragmented global digital landscape.
- **New Alliances:** Cooperative frameworks, like the US-EU Trade and Technology Council, are emerging to align transatlantic 5G and technology policies[14].
- **Preparation for 6G:** Geopolitical divisions in 5G deployment will likely influence subsequent generations, with standard-setting, intellectual property, and vendor ecosystems growing more politicized[14][12].

CONCLUSION

5G networks promise transformative societal and economic benefits but are also reshaping global power dynamics. Regulatory frameworks are increasingly shaped less by technical standards and more by security imperatives and geopolitics. The future of 5G—and, ultimately, 6G—will depend on nations' ability to balance innovation, security, and collaboration, amid a landscape defined by suspicion, competition, and strategic ambition.

[image:1]

[image:2]

REFERENCES:

1. https://wraycastle.com/blogs/knowledge-base/understanding-5g-regulation-what-it-means-for-you-and-your-devices-1
2. https://www.numberanalytics.com/blog/5g-regulation-telecom-perspective

3. https://wraycastle.com/blogs/knowledge-base/understanding-5g-regulation-what-it-means-for-you-and-your-devices
4. https://www.euronews.com/next/2024/08/12/eleven-eu-countries-took-5g-security-measures-to-ban-huawei-zte
5. https://www.euractiv.com/section/tech/news/seventeen-eu-countries-not-ready-to-cut-china-5g-dependence/
6. https://www.tcs.com/what-we-do/services/cybersecurity/white-paper/5g-technology-network-security
7. https://www.entrust.com/blog/2023/10/5g-security
8. https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era/
9. https://www.mastercard.com/news/perspectives/2021/5g-and-the-politics-of-change-could-nationalism-erode-innovation-and-economic-growth/
10. https://en.wikipedia.org/wiki/Concerns_over_Chinese_involvement_in_5G_wireless_networks
11. https://teletimesinternational.com/2023/5g-future-international-relations/
12. https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/nocetti_5g_europe_2022_us.pdf
13. https://en.wikipedia.org/wiki/5G
14. https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2025/ui-brief-no.-3-2025-6g-geopol-bjorn-f.pdf