The significance of technology in the contest between the United States and China

Błażej Sajduk, PhD
(Assistant Professor, Department of National Security, Jagiellonian University and Deputy Head, Center for Quantitative Political Science, Poland)

Publication date: 27 August 2023

It is becoming increasingly evident that technology will wield substantial influence within the ongoing competition between the United States and China, contributing significantly to the tensions on the geopolitical stage. The race to establish universally accepted technological standards has the potential to serve as a viable complement or even alternative to economic sanctions. Given that the current era of globalization hinges on shared standards for information exchange, the rise of incompatible solutions could expedite the process of deglobalization. Consequently, distinct regions might arise across the world that are not only politically connected but also technologically aligned with specific centers of influence.

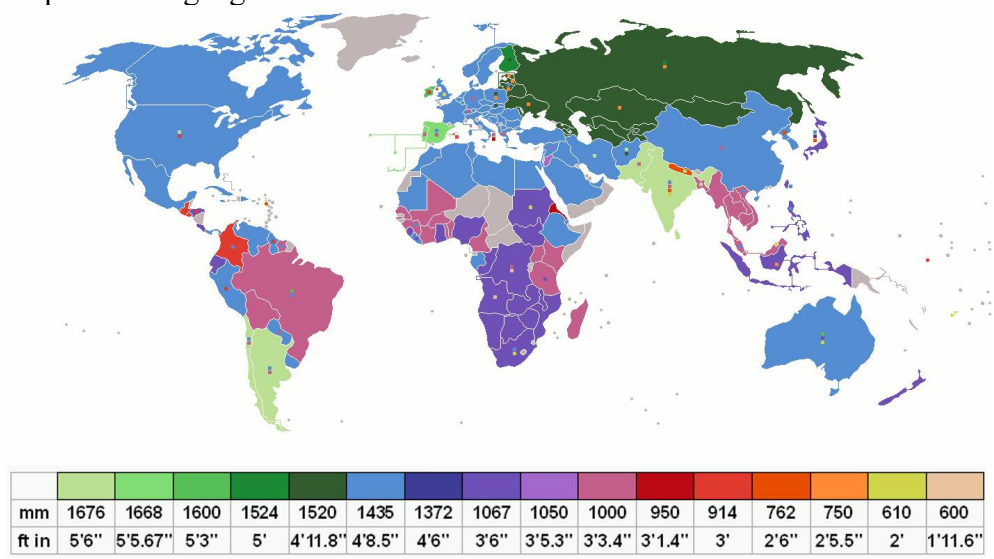
Analogous to the Cold War era, a polarity is set to emerge—one propelled by democratic nations with the United States at its core and the other influenced by nations aligned with China, leveraging the technological innovations it provides. In the ensuing discourse, the significance of technological standards will be explored, along with the examination of two pivotal arenas of technological rivalry between the USA and China: the trajectory of global Internet governance and the evolution of the 5G network. Both realms possess the potential to transform into spaces where the rivalry between the United States and China could result in a technological divergence, ultimately giving rise to regions that exhibit greater technological integration with one of the opposing factions.

The Significance of Technical Standards

The role of technical standards may be exemplified through two instances. The first pertains to the varying plugs used for electrical sockets – a familiar experience for those traveling between continental Europe, the UK, and the US, as it requires adapters to connect devices to differing socket types to ensure seamless operation. This aspect's potential for manipulation is reminiscent of the situation with railway gauges. Since the 19th century, the majority of rail networks in Europe have embraced the British-designed rail gauge (1,435 mm); however, Russia's chosen rail gauge surpasses that of many neighboring nations (1,520 mm). Moscow's

decision in this context likely stemmed from security considerations, aiming to impede enemy transportation during times of conflict.

Map 1. Track gauge.



mm	1676	1668	1600	1524	1520	1435	1372	1067	1050	1000	950	914	762	750	610	600
ft in	5'6"	5'5.67"	5'3"	5'	4'11.8"	4'8.5"	4'6"	3'6"	3'5.3"	3'3.4"	3'1.4"	3'	2'6"	2'5.5"	2'	1'11.6"

Source: https://upload.wikimedia.org/wikipedia/commons/1/1f/Rail_gauge_world.png

In the realm of modern telecommunications technologies, matters are governed by various supranational entities known as Standard-Setting Bodies (SSBs)[1]. What is worth noting is the fact that China continues to implement its strategy entitled 'Standards 2035'[2] with a primary objective of enhancing not only the quality of its domestic technological solutions but also its influence over global standards. Notably, some of these SSBs have been overseen by individuals of Chinese nationality[3].

During the 1980s and 1990s, the technology industry witnessed a phenomenon termed 'standards wars.' However, during that era, the rivalry primarily revolved around private corporations endeavoring to sideline competitors by creating incompatible solutions[4]. Over time, these conflicts largely waned due to the business rationale that strongly advocates for the interoperability of solutions, thereby promoting the forces of globalization. Presently, within the context of the escalating rivalry between the United States and China, the

[1] Including mainly the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

[2] Yi Wu, *China Standards 2035 Strategy: Recent Developments and Implications for Foreign Companies*, 26 06 2022, https://www.china-briefing.com/news/china-standards-2035-strategy-recent-developments-and-their-implications-foreign-companies/.

[3] Nonetheless, there has been a recent shift in this landscape, demonstrated by the appointment of Doreen Bogdan-Martin from the USA as the head of the ITU. See. Member States elect Doreen Bogdan-Martin as ITU Secretary-General, 29 09 2022, https://www.itu.int/en/mediacentre/Pages/PR-2022-09-29-ITU-SG-elected-Doreen-Bogdan-Martin.aspx.

[4] See. Carl Shapiro, Hal R. Varian, *The Art of Standards Wars*, California Management Review 1999, vol. 4 no. 2, https://faculty.haas.berkeley.edu/shapiro/wars.pdf.

'standards wars' could reignite with heightened intensity, involving both state-owned Chinese enterprises and private entities enjoying substantial backing from the United States.

The Internet vs. Internets

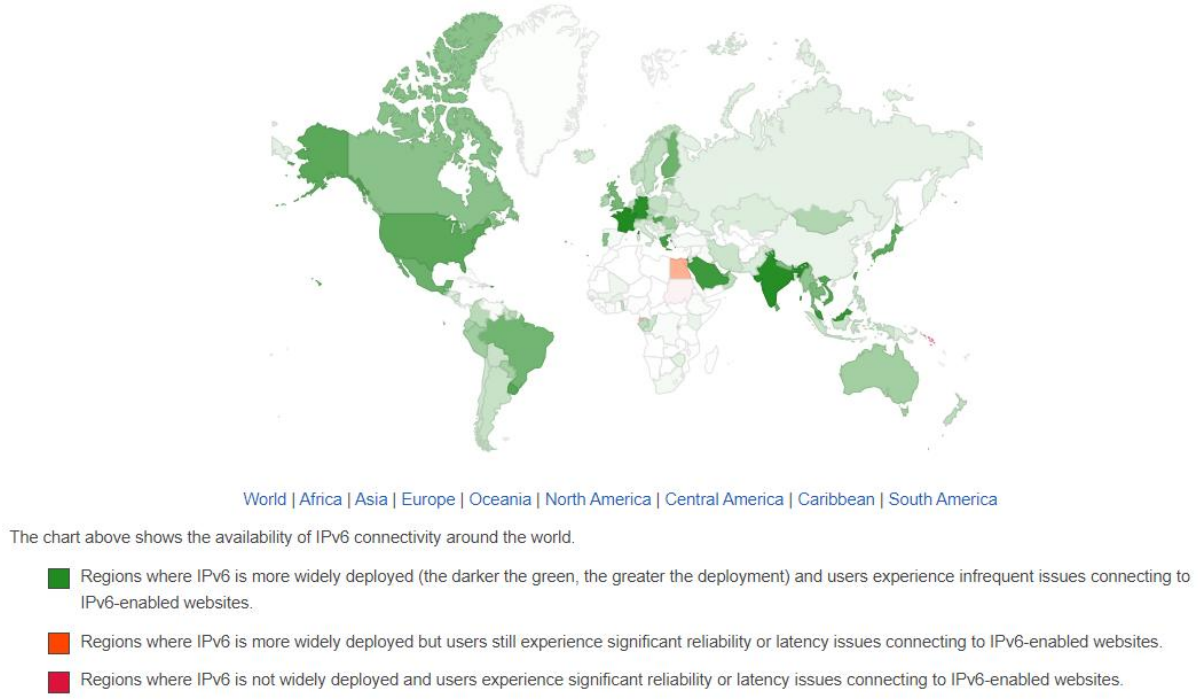
The emergence of digital spheres of influence is closely associated with the looming threat of a phenomenon known as Spliternet – the further division of the global Internet into smaller sub-networks that would be controlled by central authorities within national borders. Such an approach has been in effect for some time in China and Russia; however, it might increasingly become a model adopted by other nations, particularly those interested in implementing 5G technology from Huawei, the Chinese tech giant. It's worth recalling that the dispute over who should manage the Internet has been ongoing for years and is most notably observable within the United Nations (UN), where two distinct visions clash.

The first vision, championed by the USA and like-minded countries, advocates for the current model of Internet governance through transnational multistakeholder organizations, notably including the Internet Corporation for Assigned Names and Numbers (ICANN). The second vision contends that national governments should oversee their own 'Internets', a concept endorsed by countries such as Russia and China. These differences of opinion have led to the coexistence of two parallel bodies within the UN, both addressing the same issue – the regulation of international law norms within cyberspace[5]. As of now, consensus on the future of global Internet governance has proven elusive.

Currently, with the proliferation of devices constituting the Internet of Things (IoT), there's a need to transition to a newer version of the internet protocol responsible for data exchange in the network. The world is presently in the process of transitioning from the old protocol (IPv4), which enabled the connection of 4.3 billion addresses, to the new (IPv6), allowing for the connection of a staggering 340 sextillion addresses. The implementation status of the new internet protocol version is uneven across the globe, with African countries notably lagging behind in this process (refer to Map no. 2).

Map 2. Per-Country IPV6 adoption.

[5] The first is The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, established in 2003, supported mainly by Western democracies. The second body is the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security, supported mainly by Russia, China and countries that do not always respect the rules of democracy.



Source: https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption.

An important point to underscore is that between 2018 and 2020, Huawei advocated for its proprietary concept known as 'New IP' within international forums tasked with overseeing telecommunications frameworks, including the ITU. Numerous experts, particularly from Western nations, highlight concerns about Chinese innovations potentially jeopardizing privacy due to their capacity for deep packet inspection and individual identification on the Internet. Notably, Huawei has been notably proactive in propagating its proprietary solution among nations in the Arab[6] and African[7] regions.

5G network

The matter concerning the incorporation of offerings from Chinese corporations (such as Huawei and ZTE) into the development of the 5G network garnered significant media attention. Due to the exerted pressure from successive US administrations led by both Donald Trump and Joseph Biden, the United States successfully persuaded the majority of its partners to abstain from incorporating Chinese 5G solutions into their networks and to remove them from existing 4th and 3rd generation networks. Despite this, nations across South America, Africa, and the majority of Asia actively opt for Chinese telecommunications solutions, which are often more cost-effective compared to Western alternatives[8].

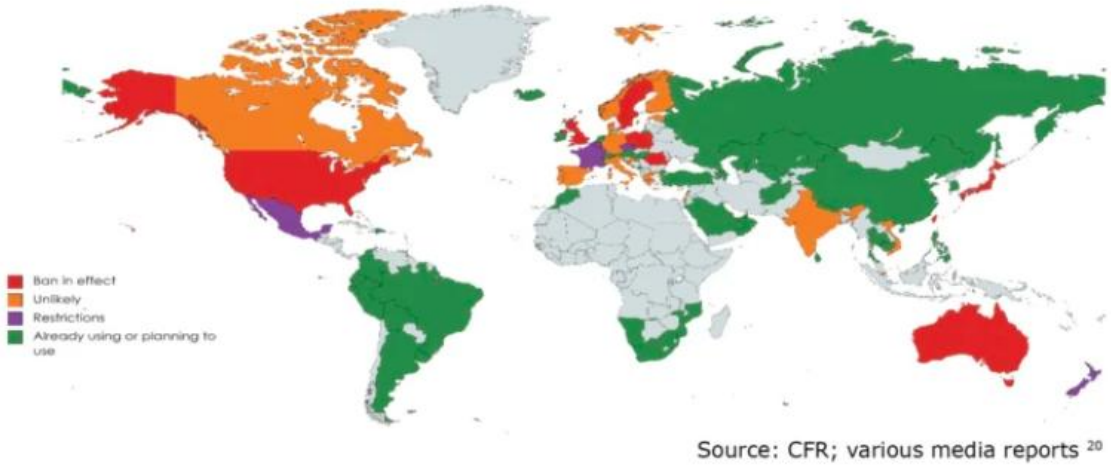
---

[6] *AICTO and Huawei promote IPv6 development in the Arab region*, 4 07 2023, https://www.theregister.com/2023/07/04/aicto_huawei_ipv6_cooperation/.

[7] *Huawei Launches the First IP Club Member Program in Africa to Accelerate Africa's Industry Digital Development,* 31 05 2023, https://e.huawei.com/en/news/2023/solutions/enterprise-network/first-ip-club-member-program.

[8] This pertains not only to mobile networks or the Internet but also encompasses the Chinese Beidou terrestrial positioning system, serving as an alternative to the Global Positioning System (GPS).

Map 3. Global Response to Huawei's 5G mobile networks



Source: https://www.cis.org.au/publication/dealing-with-the-digital-yuan-policy-choices-facing-australia/.

Within the realm of 5G technology, the IT facet concerning the potential for error correction during signal transmission holds noteworthy significance. Presently, global bodies of experts responsible for devising technical specifications for 5G technology, including 3GPP, have reached a consensus on the admissibility of two concurrent solutions. The first solution, cultivated over an extended duration, includes options like the low-density parity check (LDPC) widely pursued in the West. It's important to highlight that in this context, numerous companies possess internationally recognized patents, without a singular frontrunner.

The second sanctioned standard entails what is termed as 'the polar codes', developed with substantial support from China. Notably, a majority of the patents in this realm are held by Huawei (approximately 23%)[9], a company vigorously engaged in advocating for the integration of this solution in forthcoming global 5G implementations. Evidently, this technological domain presents an avenue that could potentially be leveraged to constrain the interoperability of future solutions.

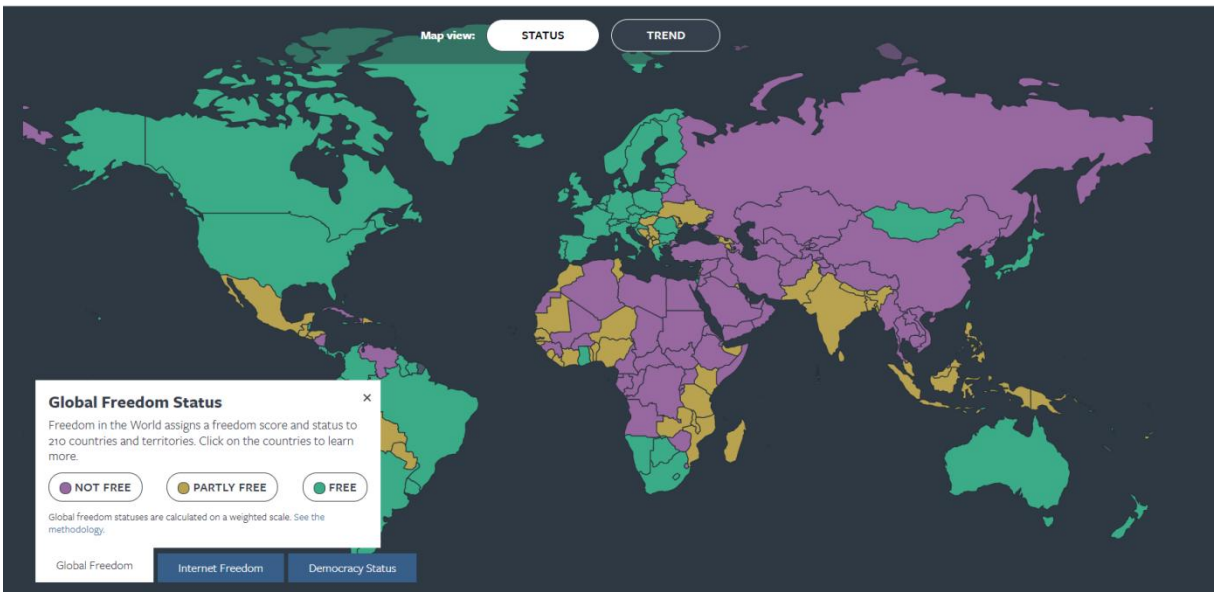
Conclusion

The resurgence of Cold War-era divisions appears increasingly probable in a 21st-century context. Beyond mere political alliances, the technological domain is poised to assume a pivotal role. Over recent years, technology has shed its status as a neutral territory, as policymakers now regard it as a realm ripe for geopolitical maneuvering. Nations are compelled to make choices and dismiss certain options driven by (geo-)political motives. The subsequent phase in the rivalry between these opposing factions might involve the strategic utilization of technological standards to curtail the interoperability of adopted solutions. This

[9] Dimitris Mavrakis, 5G NR Coding Schemes: A New Start with a Long History, 20 07 2020, https://www.abiresearch.com/blogs/2022/07/20/5g-nr-coding-schemes-a-new-start-with-a-long-history/.

potential trajectory represents a disconcerting form of competition, as nobody would reasonably wish to bear witness to a global conflict entangling two superpowers.

Source 4. Map of Global Freedom



Source: https://freedomhouse.org/explore-the-map?type=fiw&year=2023.

Considering only the above information, it is clear that there is a subsoil within the technological rivalry for use in the future phase of the geopolitical rivalry between China and the US. The outline of the future spheres of competition is helped by the map illustrating the level of freedom, which is developed each year by The Freedom House (see map no. 4). It clearly shows that countries with lower scores (in which societies do not live fully democratic systems) are often countries that are more willing to adopt Chinese technological solutions, and more willing to support Chinese diplomatic initiatives. In the future, it will be particularly interesting to follow the policies of countries that do not clearly fit into the category of democracies excluding Chinese technologies (e.g. Brazil) and which are not fully democratic but exclude Chinese solutions (e.g. India). Countries that are (non-democratic) allies of the US that accept Chinese solutions (e.g. Saudi Arabia, Turkey) will constitute a separate group of cases.