Making Sense of Technological Spheres of Influence

VALENTIN WEBER

STRATEGIC UPDATE
APRIL 2020

LSE Ideas

Ranked #1 university affiliated think tank in the world in the 2019 *Global Go To Think Tank Index*.

LSE IDEAS is LSE's foreign policy think tank.
We connect academic knowledge of diplomacy and strategy with the people who use it.

Through sustained engagement with policymakers and opinion-formers, IDEAS provides a forum that informs policy debate and connects academic research with the practice of diplomacy and strategy.

IDEAS hosts interdisciplinary research projects, produces working papers and reports, holds public and off-the-record events, and delivers cutting-edge executive training programmes for government, business and third-sector organisations.

lseideas lseideas

Making Sense of Technological Spheres of Influence

VALENTIN WEBER

THE AUTHOR

Valentin Weber is a DPhil Candidate in Cyber Security at the Centre for Doctoral Training in Cyber Security and a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. Previously, he was an Open Technology Fund Senior Fellow in Information Controls at the Berkman Klein Center for Internet & Society, Harvard University. His interests lie in strategy, grand strategy, information controls, and more generally, the politics of cyberspace. His main research focus is on the United States, China, and Russia.

On 28 January 2020, the United Kingdom (UK) announced that Huawei will be allowed to build part of the country's 5G core network. The United States (US), citing Huawei equipment's high-risk nature to critical infrastructures, responded with threats of restricting intelligence cooperation. A few months earlier, 15,000 kilometres to the southeast, Australia announced that it would exclude Chinese equipment from its 5G networks, unsurprisingly prompting outcry and threats from China.[1] The UK appears not to have bought into the concept of "technological spheres of influence," while Australia has. Australia's actions should decrease Chinese control over technology there through exclusion; UK actions should allow for a mixed technological environment within its territory.

Although controlling technology and its supply remains important, the fight over technological governance is equally crucial. Since the early days of the Internet, the US has advocated placing companies and non-state actors at the core of technological and Internet governance, while China has always advocated for a strong state role. Both China and the US have also always pushed for their visions to be adopted by other states: the US through its Internet freedom agenda and China via its concept of Internet sovereignty.[2]

The US's and China's vying for technological influence has brought about the emergence of technological spheres of influence. These technological spheres of influence are geographical areas in which an external power has *privileged* but not *exclusive capability to control* technology and/or where the external actor exerts predominant influence in terms of technology governance.

The term *sphere of influence* is a product of geopolitics. The British politician Lord Curzon purportedly first used the term in the mid 19th century, crediting the Russian foreign minister for mentioning it in relation to Afghanistan.[3] Throughout history, technology has played a fundamental role in the practice of geopolitics—predominantly as an enabler of land or sea power. In the 21st century, as the Internet and associated technologies (hard infrastructure, Internet-of-things devices, smartphones) are now at the centre of what constitutes influence, the geopolitical importance of technology continues to grow. These new realities warrant an examination of what technological spheres of influence are.

> These *technological spheres of influence* are geographical areas in which an external power has privileged but not exclusive capability to control technology and/or where the external actor exerts predominant influence in terms of technology governance.

PRIVILEGED CAPABILITY TO CONTROL TECHNOLOGY

One has to assume that the US and China have the capability to control every state's Internet-connected technology, if they wish so. They might have greater sway over some states, such as the US over the UK and Japan, or China over Thailand and Malaysia, because these states rely more heavily on one or the other superpower for their technology procurement. If many critical components of a nation's 5G Internet infrastructure, hardware, and software are of US and/or Chinese origin, it gives the US and/or China easier access to snoop or disrupt that country's online communications.[4] Being a key technology supplier allows the supplier privileged capability to control a customer state. This was seen in the recent revelations that the US and German intelligence agencies owned Crypto AG, a Swiss cryptographic equipment maker, which allowed them to snoop on dozens of countries.[5] The US used this capability to spy on Argentinian communications during the Falklands War (shared with the UK) and Iranian leaders during the hostage crisis, thus demonstrating how control over technology can enhance other forms of statecraft.[6] Still, this privileged capability to exert control is not exclusive. A Cisco router may give the US a head start in hacking a device, but this does not prevent Iran or China from gaining access as well.

There are only a few places trending towards becoming exclusively Chinese or US technospheres. Thailand, for instance, has moved towards strongly relying on Chinese technology, while Japan has shunned Chinese technology.

PREDOMINANT INFLUENCE IN TERMS OF TECHNOLOGY GOVERNANCE

The spheres of technological governance have become more exclusive. Norway, for instance, is an adherent to the US approach of allowing non-state actors and private companies to govern technology and the Internet. In adhering to the US model, Norway also accepts US-promoted norms, such as Internet freedom. As a result, both in practice and in principle, Norway falls within the US' sphere of influence, and it is unlikely that this will change any time soon.

VARYING DEGREES OF INFLUENCE: CORE AND PERIPHERY OF TECHNOSPHERES

Most countries are within the US and Chinese peripheral technospheres. In the periphery, the respective hegemon has privileged capability to control devices abroad due to its dominant technological supplier status. And yet, the US and China have little influence over technology governance here. For example, while the US may be able to easily exploit critical parts of Thailand's Internet infrastructure, it has little influence over Thailand's approach to Internet governance, whose cyber security laws and content controls largely mimic China's environment. Indeed, China and the US have both privileged control over technology and hold considerable influence over how technology is governed in a small but increasing number of states. These states fall within the US/Chinese core technospheres (See the below analysis of Thailand and Japan as examples of core technospheres).

NO MUTUAL RECOGNITION OF RESPECTIVE TECHNOSPHERES

Historically, an important attribute of spheres of influence has been the mutual understanding amongst great powers of whose spheres of influence are situated where.[7] There was, for example, little risk for Cold War-era escalation within Eastern

Concentric circles of influence

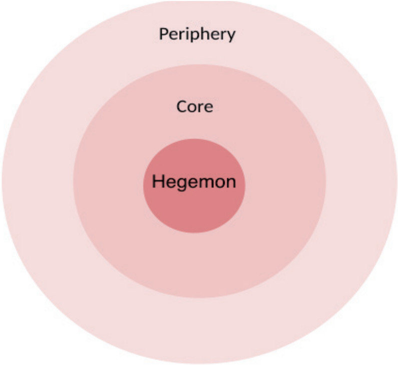


Figure 1. Concentric circles of influence consist of the hegemon, the core and the periphery of its technosphere.

Europe because both the US and Soviet Union understood this to be the latter's sphere of influence.[8] Hence when there was an uprising, the US did not openly intervene to foster further protests. In the digital realm, however, there is only sparse recognition of mutual technospheres. Indeed, both China and the US have threatened Germany, one example of a disputed technosphere, with sanctions as the country decides about core 5G mobile infrastructure.[9]

THE MOST PRIZED TECHNOSPHERE: THE TECHNOLOGICAL CRESCENT

Many geostrategists have placed Eurasia at the centre of history's geopolitical pivot. Throughout history, this swath of land has harboured major geopolitical players, from the Romans to the Mongols to the Manchus. Each empire used the area's abundant resources to acquire immense power—with the western, southern, and eastern fringes being especially vital, as Nicholas Spykman observed in the middle of the twentieth century.[10] This paper, therefore, designates the combination of Europe, South(east) Asia, and East Asia as the world's *Technological Crescent*, the most prized territory over which great powers are seeking to gain influence. It contains states with important rare earth resources (China, India, Malaysia, Myanmar, Thailand, and Vietnam), which are used to produce high-tech products.[11] It also plays host to the world's technology supply chain and innovation hubs, spanning from China, Taiwan, South Korea, Japan, Thailand, through to Germany, France, and the UK. In addition, the territory houses companies such as ARM, BBK Electronics, Bosch, Foxconn, Fujitsu, Huawei, Infineon, Samsung, Siemens, as well as cyber powers like Iran and Israel.

The *Technological Crescent*'s geopolitical importance also bears more traditional characteristics. It is here that two of the three largest economic, military, and technological political entities—China and the EU—interact. It is more critical of a geographical pivot than the Eurasian hinterland. Russia, the preeminent power there, while still important (especially regarding its cyber-attack and information warfare capabilities), is a waning power with an economy the size of Italy's and almost no companies that provide technology or services beyond its borders. It is thus increasingly apparent that Russia and the region at large—which includes states such as Kazakhstan, Mongolia, and Uzbekistan—do not represent the most vital technological area.

ANALYSING US AND CHINESE TECHNOSPHERES WITHIN THE TECHNOLOGICAL CRESCENT

The following section examines states at the eastern, southeastern, and western fringes of the Crescent—Japan, Thailand, and the UK—and analyses how they fit in the respective US and Chinese technospheres. It is evident that neither China nor the US have yet gained a dominant influence in the Crescent, largely because the geographical area is too technologically and governmentally mixed.

Japan is at the core of the US technosphere and is, unsurprisingly, one of the few countries that entirely prohibited Huawei and ZTE from providing its 5G infrastructure. Japan, in this respect, followed the US's decision to ban the two Chinese providers from supplying critical technology, citing national security concerns. This evinces an intentional technological decoupling from China, leaving behind technology largely produced by South Korean, Southeast Asian, and American or European companies.

At the same time, Japan remains a staunch advocate of a multi-stakeholder model of Internet governance and online freedoms domestically and internationally, following the US-promoted norm of regulating Internet-connected technology.

Thailand, for its part, is increasingly switching away from US technology, thanks largely to Chinese economic incentives that have enticed Bangkok to adopt Beijing's preferred hardware and software. In fact, a whole new Chinese-provided technological ecosystem—one built to be independent from the US—is emerging in Thailand. This ecosystem spans 5G infrastructure, a satellite network, surveillance systems, and deepened research cooperation. Huawei is already on the way to becoming a monopolistic mobile Internet supplier.[12] China also provides substantial surveillance equipment to Thai police and government authorities.[13] In 2013, Thailand reached a $297 million agreement with China to foster the utilisation of China's satellite navigation network, Beidou, in Thailand's transport sector, for its disaster relief, and power distribution.[14] Expanding Beidou's footprint in Thailand is ultimately part of China's larger aim to extend the Beidou Navigation Satellite System's reach by 3000 miles, far into Southeast Asia and South Asia, with both commercial and military applications. Beidou hopes to increase the accuracy of internet of things (IoT) device location independently from the US's Global

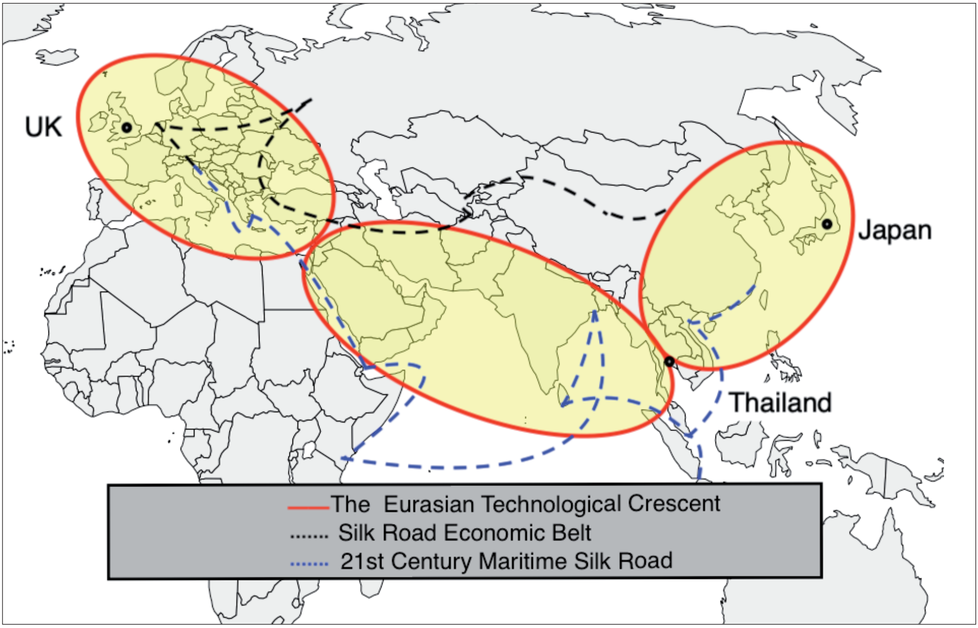
> "It is likely that US-China competition will, in the short term, focus on larger and pivotal Eurasian states—such as Germany, France, Japan, and South Korea—aiming to draw them deeper into their respective *technospheres*."

Positioning System (GPS).[15] Concurrently, Thailand's regime has continuously cracked down on its political opposition and is one of the worst countries in terms of online freedoms.[16] Bangkok is here mirroring Beijing, imposing a very state-centric system that relies heavily on censorship and repressive cyber security laws.

Additionally, the United Kingdom rejects the concept of exclusive technospheres, believing instead that the international technological landscape is better off with a panoply of suppliers and providers. London continues to prioritise economic competition over national security posturing, contending that the imposition of safeguards can mitigate any risks. The UK, in this sense, does in practice reflect the belief of the US Principal Deputy Director of National Intelligence Susan Gordon, that "you have to presume a dirty network."[17] In this vein, the capping of the market share of a high-risk supplier is reasonable. The UK does, however, also strongly rely on Chinese-produced surveillance equipment. There is less clarification as to how potential security breaches would be countered on this front. Little is known, for instance, about how the UK mitigates risks that come with the Hikvision equipment that is installed in London's boroughs of Kensington, Hackney, Camden, and used by police, universities, and hospitals throughout the country.[18]

> "The current technological supply chains are so deeply intertwined that further decoupling would be very costly."

Still, the UK, while refusing to become too reliant on one great power for technology procurement, is one of the most active advocates for freedoms online and a governance model of Internet-connected technologies that relies on non-state actors. It has long pushed this agenda, most notably with a pioneering conference on cyberspace in 2011 that aimed to further online freedoms.[19] In short, UK actions and discourse are a flagship example of multi-stakeholderism.


UK
Japan
Thailand
The Eurasian Technological Crescent
Silk Road Economic Belt
21st Century Maritime Silk Road

Map 1. Note how China's land and maritime silk roads enclose the Eurasian Technological Crescent from the North and South.[20]

THE FUTURE OF TECHNOSPHERES

Future technosphere development remains very much open. One possibility is a global bifurcation into two technospheres. In this scenario, countries such as Japan, Australia and New Zealand choose to rely on US technology, and to a lesser extent on some European providers such Ericsson and Nokia, while states such as Iran and Russia actively remove US-produced components from their networks and replace them with native or Chinese-built ones, citing national security concerns. Other states may be driven into American or Chinese technospheres by financial incentives. Malaysia and Thailand do not rely on China because of their hostility towards the US but rather because of the cheapness of Chinese technology, which often comes concurrently with development aid and Belt and Road Initiative infrastructure projects. A bifurcation is especially likely if China and the US increasingly pressure these states to pick sides.[21]

It is likely that US-China competition will, in the short term, focus on larger and pivotal Eurasian states (such as Germany, France, Japan, South Korea), aiming to draw them deeper into their respective technospheres. If these states choose to do so, it will have a ripple effect on smaller states. However, if these pivotal states resist US and Chinese pressure, they may prevent a global technospherical bifurcation.

Such bifurcation should be avoided. The current technological supply chains are so deeply intertwined that further decoupling would be very costly. Indeed, as it became apparent during the 5G debate, excluding Huawei and ZTE from supplying equipment would shut out 40 percent of the competition. This would likely have pecuniary disadvantages for customer countries.[22] Fewer technological competitors would ensure diminished competition in the cyber security market.

For all the above reasons, larger and/or pivotal states in Eurasia (e.g. France, Germany, etc.) should work towards preventing the further emergence of technospheres. Accordingly, these countries should help countries resist US and Chinese pressure. European actors could accomplish this by establishing a continental body to vet technologies of critical importance and impose a cap on the market share of those suppliers likely to dominate.

In terms of technological governance, however, factionalization will likely deepen. States that otherwise resist technological bifurcation within their country (e.g. the UK) are strongly placed in the multi-stakeholder group of countries when it comes to the governance of technology. Although states may be unwillingly caught between Chinese and American pressures, there is almost no resistance to establishing two zones of thinking about the governance of technology—one where the state is at the centre of power and another where a group of stakeholders such as private companies and individuals hold power concurrently with the state. The increasing popularity of the former state-centric model is worrisome given that this system is generally accompanied by a deterioration of citizens' fundamental freedoms. To counter this challenge, countries that subscribe to the multi-stakeholder model should draft a strategic narrative that highlights their model's advantages in comparison to the state-centric model. At the same time, they should focus on crafting a legal framework for governing emerging surveillance technologies that protects the rights and privacy of citizens. In other words, they should lead by example. ■

ENDNOTES

[1] Qingqing Li, "Australia to Pay for 5G Restrictions on Huawei," *Global Times,* April 15, 2019, http://www.globaltimes.cn/content/1146018.shtml.

[2] See the following resources for a deeper analysis of how the global presence of U.S. and Chinese visions of governance translates into influence abroad: Shawn M Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* (Urbana, Chicago, and Springfield: University of Illinois Press, 2015); Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," *Centre for Technology and Global Affairs, University of Oxford*, September 2019, https://ctga.web.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrols.pdf.

[3] George Nathaniel Curzon, 1st Marquess Curzon of Kedleston, *Frontiers* (Oxford: Clarendon press, 1907).

[4] Bruce Schneier, "5G Security," January 14, 2020, https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html.

[5] Sean Gallagher, "For Decades, US and Germany Owned Swiss Crypto Company Used by 120 Countries," *Ars Technica*, November 2, 2020, https://arstechnica.com/tech-policy/2020/02/us-german-intel-owned-swiss-crypto-used-by-dozens-of-countries/.

[6] Ibid.

[7] Paul Keal, "Contemporary Understanding About Spheres of Influence," *Rev. Int. Stud.* 9, no. 3 (1983): 155–72.

[8] Ibid.

[9] Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers," *The New York Times*, January 16, 2020, https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html.

[10] This geographical space was designated by Halford Mackinder as the Inner or Marginal Crescent and by Nicholas Spykman as the Rimland.

[11] US Geological Survey, "US Geological Survey, Mineral Commodity Summaries - Rare Earths," February 2019, https://prd-wret.s3-us-west-2.amazonaws.com/assets/palladium/production/atoms/files/mcs-2019-raree.pdf.

[12] Rob Schmitz, "Thailand Moves Forward With Chinese Tech Company Huawei To Build 5G Network," *NPR.Org*, March 27, 2019, https://www.npr.org/2019/03/27/707358090/thailand-moves-forward-with-chinese-tech-company-huawei-to-build-5g-network.

[13] Weber, "The Worldwide Web of Chinese and Russian Information Controls."

[14] Stephen Chen, "Thailand Is Beidou Navigation Network's First Overseas Client," *South China Morning Post*, April 4, 2013, https://www.scmp.com/news/china/article/1206567/thailand-beidou-navigation-networks-first-overseas-client.

[15] Shunsuke Tabeta, "China Decouples From US in Space With 2020 'GPS' Completion," *Nikkei Asian Review*, accessed January 31, 2020, https://webcache.googleusercontent.com/search?q=cache:DmwswP4Da5UJ:https://asia.nikkei.com/Business/China-tech/China-decouples-from-US-in-space-with-2020-GPS-completion+&cd=13&hl=en&ct=clnk&gl=uk.

[16] Human Rights Watch, "Thailand: Court Dissolves Opposition Party," February 22, 2020, https://www.hrw.org/news/2020/02/22/thailand-court-dissolves-opposition-party; Freedom House, "Thailand," 2020, https://freedomhouse.org/country/thailand/freedom-world/2020.

[17] Schneier, "5G Security."

[18] Ryan Gallagher, "Cameras Linked to Chinese Government Stir Alarm in UK Parliament," *The Intercept*, April 9, 2019, https://theintercept.com/2019/04/09/hikvision-cameras-uk-parliament/.

19 United Kingdom Foreign and Commonwealth Office, “London Conference on Cyberspace: Chair’s Statement,” *GOV.UK*, November 2, 2011, https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement.

20 The location of the Crescent is approximate (fluid) and can vary throughout the years. States can be added or removed from it, depending on whether they harbour considerable technological resources. The representation of the Crescent is meant to indicate the larger geographical areas of importance and not a detailed list of which states are part of it or not.

21 U.S. Department of State, “A Free and Open Indo-Pacific: Advancing a Shared Vision,” November 4, 2019, https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf

22 Valentin Weber, “Finding a European Response to Huawei’s 5G Ambitions” (The Norwegian Institute of International Affairs, March 2019), https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2591639/NUPI_Policy_Brief_5_2019_Weber.pdf?sequence=2&isAllowed=y.

LSE THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

EXECUTIVE MASTERS PROGRAMME

INTERNATIONAL STRATEGY AND DIPLOMACY

LSE IDEAS, a Centre for the study of international affairs, brings together academics and policy-makers to think strategically about world events.

This one year **EXECUTIVE MASTERS PROGRAMME** is at the heart of that endeavour. While studying in a world-leading university you will be able to learn from top LSE academics and senior policy practitioners.

The programme will sharpen your ability to challenge conventional thinking, explore new techniques for addressing risk and threats, and coach you in devising effective strategies to address them.

The course has been especially tailored so that you can accelerate your career while holding a demanding position in the public or private sector.

"Right from the first week I was able to apply the lessons I had learnt to our operational and policy work and to coach my teams to look at issues differently."

– **Karen Pierce**
British Ambassador
to the United Nations

CONTACT US

ideas.strategy@lse.ac.uk
+44 (0)20 7955 6526
lse.ac.uk/ideas/exec

Making Sense of Technological Spheres of Influence

VALENTIN WEBER

The deterioration of Sino-American relations and the rise of novel forms of statecraft have given way to a worrying new feature of the international system: ***technological spheres of influence***. In this Strategic Update, Valentin Weber explains how we have arrived at this novel geopolitical arrangement, where in the world the greatest contestation lies, and what the future of ***technospheres*** may hold.

For general enquiries:

LSE IDEAS
Floor 9, Pankhurst House
1 Clement's Inn, London
WC2A 2AZ

☎ +44 (0)20 7849 4918

✉ ideas@lse.ac.uk

lse.ac.uk/ideas

@lseideas

lseideas

Cover image:
www.vexels.com