Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace

Shubh Gupta

PhD Scholar, Centre for Studies in Science Policy, Jawaharlal Nehru University. Address: 212 Chandrabhaga Hostel, Jawaharlal Nehru University, New Mehrauli Road 110067, New Delhi, India. E-mail: Shubhgupta008 @gmail.com

Reeta Sony A.L.

Assistant Professor, Centre for Studies in Science Policy, Jawaharlal Nehru University. Address: Warden Flat N0. 4, Godavari Hostel, Jawaharlal Nehru University, New Mehrauli Road 110067, New Delhi, India. E-mail: reetasony@mail.jnu.ac.in

Abstract

The dawn of the neocolonial project has seen the emergence of a new space: data. Data is a raw material that can be stitched, processed and marketed in the same way as the East India Company (EIC) used to do with India's cotton. EIC, which started as one of the world's first joint-stock companies, turned into a wild beast, building a corporate lobby with the help of lawyers and MP shareholders to amend legislation in its favor. The EIC became a particularly atrocious and innovative colonial project that directly or indirectly controlled continents, thanks to an army larger than the army of any nation-state at the time. The Drain Theory of Dadabhai Naroji have opened India's eyes to how the EIC was taking raw material from the country and converting it into a finished product that was marketed in India again in the same way as raw data is being processed outside India and then marketed here today. In today's digital era, big corporations need not own big armies, as companies are protected by nation-states and bailed out when required. Today, one does not need to travel overseas to explore and conquer Gold, God and Glory; instead, they are a click away. The neocolonial project runs on digital platforms, while the popular narrative of bridging the digital divide and giving internet access to millions of people resembles the idea of the "white savior" liberating the "noble savage" through modern Western education. Facebook's grand plan of providing free internet to all can be best understood as a neocolonial strategy to mine the data of billions by equating it with water and land. Similarly, the Cambridge Analytica scandal provides an example of how neocolonial forces can influence the fundamental democratic process of electing a government. Therefore, nations endorsing democratic values should be especially wary of the trap of neocolonialist forces, as such nations are particularly vulnerable to their project. This paper critically study the cyber security infrastructure and policies in India and analyze the India's approach towards cyber sovereignty and data colonialism and thereafter examine the India's strategic position in cyberspace and suggest policy recommendations.

Keywords

data colonialism; cyber sovereignty; data sovereignty; cyber strategy; India's cyber strategy; India's data policy.

For citation: Gupta S., Sony R.A.L. (2021) Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace. *Legal Issues in the Digital Age,* no 2, pp. 68–81.

DOI: 10.17323/2713-2749.2021.2.68.81

Introduction

Neocolonialists view "data" as a raw material that can be stitched, processed and marketed in the same way as the East India Company once did with India's cotton. India supplied raw cotton to British mills that processed it into a finished product and resold it to British colonies [Brain J., 2021]. Britain was able to mass-produce cotton products thanks to rapid technological progress and gain a monopoly on the textile industry with the help of its imperialist policies. The finished product was much cheaper than existing products at the time and created a fashion that led the colonized to "mimic"[1] the colonialists. Even after the British physically departed from India in 1947, they left it with a colonized mindset thanks to different institutions they had created during their tyrannical rule [Preeti, 2016].

Edward Said's [2003: 1–28, 350–353] *Orientalism* shaped the discourse on post-colonialism and provided an alternative to orientalist cultural studies. Said defines orientalism as "a relationship of power, of cultural domination, the cultural equivalent of the colonialism which it accompanied" (Young R., 1995). We experience and access the power of data using the narrative perpetuated by techno-orientalists, who want to maintain the old power relationship and convert it into economic value. We have to understand that Said's work did not criticize Western knowledge; rather, it denounced the power relationships inscribed in this knowledge. Along the same lines, this chapter attempts to explore how data is seen from an Asian perspective, the power relationships it entails, and the major actors in these relationships.

The former CACI International employee Clive Humby coined the motto "*data is new oil*" (Haupt M., 2016). This narrative was pushed worldwide

[1] Bhabha H. (1984) describes how the colonial mimicry becomes a desirable trait for the colonized. For further information please refer to the citation.

to make us believe that data is like an exhaustible natural resource that will help us fuel our economy. Later, when colonized entities began to realize that, if data is indeed like oil, sovereign nations should not let tech giants extract it for free, Google introduced a new narrative that stated that "*data is more like sunlight than oil*" [Ghosh S., Kanter J., 2019]. Google wants us to believe that, like sunlight, data is a never-ending, ownerless and unperishable product that can be harvested for the improvement of humanity. As we see, whenever a nation tries to regulate its data or the internet in general, a new motto appears to make it return to the order of data colonialism.

Data, however, is neither oil nor sunlight; rather, it is a social construct or cultural object that is "embedded and integrated within a social system whose logic, rules and explicit functioning work to determine the new conditions of possibilities of users' lives" [Cheney-Lippold J., 2011: 164–181]; [Gitelman L., 2013]; [Scholz L., 2018] a specific moment in history. Data preserves and extracts individuals' social lives, turning them into inputs for an economic system that has the potential to shape our habits and practices [Dijck J., 2014: 197-208] . Thus, data has become a new means of exercising power. It is therefore important to know who possesses it.

To counter the ideology of data colonialism propagated by IT companies subtly backed by the U.S., China is pushing the opposite notion of absolute cyber sovereignty which goes against the idea of free and open internet and instead promotes its use as a tool to censor the voice of the common people [Sherman J., 2019a]. China is not the only nation to try to employ massive surveillance tools to monitor its citizen's activities online. Every country is trying to keep an eye on its citizens in one way or another, be it U.K's Karma Police [Brandom R., 2015]. India's Central Monitoring System initiated in 2013, or lawful interception and monitoring systems (LMS) [Singh S., 2013]. While every such surveillance program is run under the garb of national security, what matters is how this data is used by a sovereign nation to exercise control over its citizens and other nations.

The question then arises: which way will India choose? As of today, India is pursuing a strategy of remaining unaligned with any group and taking a flexible stance so as to assure its own interests. Nevertheless, it has the potential to serve as a model for other developing countries and conform its position as a "Vishwa Guru."[2] India can take the Gandhian approach,

[2] Vishwa Guru can be roughly translated as World's Guru(Teacher). India wants to take a role of global leadership in knowledge space based on its ancient knowledge system. Available at: https://www.dailypioneer.com/2019/columnists/the-dream-of-a-vishwa-guru.html (accessed: 03.01.2021)

making everyone learn to spin charkha and become "atmanirbhar" [Bhargava K., 2020], or it can fray its own way, as Dattopant Thengadi suggested in his book *The Third Way*, arguing that India should become neither capitalist nor socialist but rather develop its own code [Thengadi D., 1998]. India has refrained from taking extreme sides, be it in international politics or domestic economics. The rich culture of India has led it to become a mixed economy in which the interests of no person, be it a businessman or the man in the street, receive priority.

1. India's Negotiation in Cyber Space

The Indian Constitution complies with the Universal Declaration of Human Rights by guaranteeing fundamental rights to its citizens and protecting them from discrimination. It secures its citizens from border threats by other nations, guarantees food and education, protects from financial fraud, etc. Society, culture, and technology change with the passage of time, and law must adapt to these changes so that the rights guaranteed by the constitution remain intact; whenever a new artifact appears in society, it tries to influence the existing order by making institutions either adapt it or change themselves [Jasanoff S., 2004: 13–43]; [Latour B., 1987].

The exponential changes in internet technologies and the penetration of cyberspace into everyone's lifeworld [Ho W.-C., 2008: 323–342] has made governments deal with them directly rather than leaving them exclusively to scientists and technologists. Ever since Edward Snowden revealed the surveillance programs run by America's National Security Agency, the threat of the misuse of cyberspace has been felt in every nook and corner of the world, leading to a growing demand for the just and fair governance of cyberspace. This has led countries like China and Russia to reframe the idea of cyberspace and call for cyber sovereignty. The Chinese-Russian and US models are two different sides of the same coin. Instead of gravitating towards such extremes, developing countries should find a middle path that would allow their citizens to enjoy sovereignty in cyberspace [Sherman J., 2019]. In particular, India should be cautious of US tech companies that are tenaciously pushing their colonial projects in the garb of free access to their platforms. These companies use their platforms to collect raw data from users and then process and synthesize them for their benefits. In this way, public collaboration and interaction is turned into private profit. Further, these companies influence the way users connect with each other and design their platforms in a such way as to shape the social order [Dijck J. et al., 2018]. The new IT rules that try to make social intermediaries more

accountable and responsible reflect India's striving to protect individual rights and provide a just and fair environment for tech companies.

Moreover, democratic countries such as India should refrain from following the path of China, which strives for absolute cyber sovereignty. This approach allows China to exercise control over domestic politics by keeping its citizens and almost all multilateral organizations and forums under constant surveillance. China has imposed its views on developing countries, and these initiatives are being further promoted with the help of the Belt and Road Initiative (BRI) and other tools of Chinese commercial diplomacy as well as Chinese tech firms.

With 503 million internet users and the penetration of the internet into rural India due to falling prices, India ranks second in the world in data consumption [Roser M., 2018]; [Mishra D., Chanchani M., 2020]. As one of the world's top data generators, India has understood the importance of cybersecurity, leading its government to elaborate a cybersecurity policy in 2013. India has become one of the leading spokesmen for Asian and African countries on world platforms on representing and safeguarding rights to create, consume and process data. A personal data protection bill was introduced in India in 2019 to safeguard the processing of the key data of individuals; however, the final law is still being drafted. However, the country should not be lax about our cybersecurity front, as there have been repeated cyberattacks on the Indian cyber infrastructure: recently, the cybersecurity of the Kundakulam Nuclear Power Plant was breached [Madhavan N., 2019].

Having one of the highest numbers of internet users, India should urgently adopt comprehensive policies that would allow to bring any Indian or foreigner malefactor to justice. India needs to think of building its own cybersecurity infrastructure and cybersecurity policies and keep a constant watch whether it is not taking any extreme step of cyber sovereignty or data colonialism, as India plays a major role in shaping the behavior of other developing countries.

2. Understanding the importance of cyberspace in the context of national security

Let us begin by discussing why cyberspace is called "cyberspace" and not a "cyber system" or "cyber field."

In his "global cultural flows" model, A. Appadurai [Apparadurai A., 1991] defines five categories of global processes: technospace, finance space, media space, ideospace and ethnospace. These spaces are not lim-

ited by regional or national boundaries: there are multiple actors who act as nodes in a network whose flow depends on cultural practice. So, every space has its associated culture. While space is usually seen as an abstract entity or a mere receptacle of human actions [Kokot W., 2007: 10–23]. On contrary "Cultural spatiality"[3] theory treats space as a conceptualization of cultural models and a medium and product of social practice.

The space where internet operates was first called "cyberspace" in science fiction. Later, there arose the debate whether cyberspace is a social construct or an extension or evolution of existing space. It was widely accepted that cyberspace refers not to an abstract space but to a space where multiple interactions take place, leading to the definition "Cyberspace is relative, mutable, and constituted via the interactions among practice, conceptualization, and representation" [Cohen J., 2007].

When we view cyberspace as a real space, a new regulatory challenge emerges: who will regulate this space and how. The evolution of the network space is disrupting the existing nation-state conception of sovereignty.

One school of thought considers cyberspace to be a global common such as air or river and sea water. However, if it is a global common, what international laws apply to it? Who shall be responsible in the case of cyberattacks on a nation's cyberspace? Unlike natural global commons, cyberspace is a man-made common that enables the flow of data and information without barriers. If we try to constrain it within national boundaries, it will become intranet rather than internet. At the same time, critical infrastructures such as banking and defense remain within national boundaries while attacks can come from anywhere in the world, as cyberspace is borderless. Therefore, it is important to frame global laws and regulations that can help to facilitate the free flow of information.

After Edward Snowden's disclosures,[4] many developed and developing countries began to show concern about the spying taking place on the internet and its effects on their national security. A widespread demand voiced by the Chinese media was to restrict American Internet firms from the Chinese domestic market so as to protect Chinese infrastructure from

[3] Cultural spatiality theory was proposed by Hauser — Schäublin and Dickhardt in their volume "Kulturelle Räume — räumliche Kultur" [Hauser-Schäublin & Dickhardt, 2003].

[4] The National Security Agency (NSA) of United States was running a massive surveillance program codenamed PRISM, which accessed the data of leading US companies and official representatives of other sovereign Nations. The PRISM's agendas were disclosed by Edward Snowden in June 2013.

subversion [Lindsay J., 2015]. At the same time, a US Congressman charged China with establishing cyberwar rooms from which it could hurl digital bombs at other countries. There is a lot of contention in this space. Therefore, it is very important for India to think about its national interests and act more flexibly so as to facilitate its own industry rather than serving as a mere market of internet users.

3. The debate around cyber sovereignty and data colonialism

Lu Wei, then head of China's State Internet Information Office and subsequently the director of the Cyberspace Administration of China (CAC), said at the Second China–South Korea Internet Roundtable that, just as national sovereignty had been extended to seas and oceans in the 17th century and air space in the 20th century, so it will further extend to cyberspace in the 21st century [Segal A., 2020: 85–100]. Lu firmly stated that "cyberspace cannot live without sovereignty." This clearly defined China's position in cyberspace. China is propagating the idea of cyber sovereignty with all its might. This idea helps China to exercise control over its domestic politics through the constant surveillance of its citizens. China also has tremendous influence on multilateral organizations and forums as well as on developing counties with the help of its Belt and Road Initiative (BRI). At the same time, state-of-the-art Chinese tech firms and other tools of commercial diplomacy are acting as catalysts in promoting the idea of cyber sovereignty.

In short, cybersecurity has become a national priority of China, which envisages to become a cyber power by actively shaping the global internet narrative. At the 2015 World Internet Conference in Wuzhen, President of the People's Republic of China Xi Jinping said "cyber sovereignty means respecting each country's right to choose its own internet development path, its own internet management model, and its own public policies on the internet and to equal participation in international cyberspace governance. He argued that states should refrain from engaging in cyber hegemony, interfering in other countries' internal affairs, and engaging in, tolerating, or supporting online activities harming the national security of other countries". [Xi Jinping H.E., 2015]. As China is aware of its dependence on US technology firms, it is imposing restrictions on the latter in order to protect its cyber sovereignty and to develop its own firms. In September 2014, the China Banking Regulatory Commission called for 75% of ICT products used in banks to be controlled and secured by 2019 [Segal A., 2016]. The document further stated that every bank has to submit secure codes to the

Chinese government, which means creating a backdoor in all hardware and software. This was interpreted by international firms as an attempt to throw them out of the Chinese market [Mozur P., 2015].

In February 2019, the Russian Federal Assembly (Parliament) have approved the Digital Sovereignty Bill to nationalize the country's internet known as "Runet". Runet requires a separate Domain Name System (DNS), countering the hegemony of the US-backed global non-profit organization ICANN that controls global Internet DNS allocation. This will allow Russia to build an agile system that provides protection from various cyberattacks. Further, the new law also includes cross-border mobile and satellite connections in order to maintain the integrity of the network along with a system for closely monitoring all kinds of international connections and filtering them, if found suspicious. However, this law has raised numerous questions, and a large number of people have gone into the streets to protest against its limitation of internet freedom; many other people have complained about the additional control and monitoring of their internet activities. Internet access is provided only through government-licensed service providers. These providers must permit IP blocking, DNS hijacking, keyword inspection, etc. Both China and Russia have described such an approach as being effective and efficient for furthering national security and economic well-being [Venables A., 2019].

In 2017, a statement by BRICS (Brazil, Russia, India, China, and South Africa) highlighted cyber sovereignty as a key principle of international law. However, in 2018 the group declared its support for open, free and secure internet, thus promoting unfragmented global internet.

US as well as G7 and EU countries tend to view the internet as a free-flowing entity that is largely driven by market competition along with the support and regulation of the government and the participation of civil society [Basu A. et al., 2018]. However, we find historically that the narrative of *laissez-faire* has been used by the US and other capitalist countries to create new colonies based on consumption patterns. Today, data colonialism is being perpetuated under the aegis of the free market.

4. India's Emerging Role in Shaping Cyberspace Norms

India has historically played an active role in advocating the interests of the developing world at various venues such as the United Nations Convention on the Law of the Sea (UNCLOS) [Hiranandani G., 2000], the nuclear

non-proliferation regime [Kumar A., 2014], the international regime of the peaceful uses of outer space, and many more [Rao P., 2015]. Today, India has once again an excellent opportunity to play a central role in the debate about cyberspace as a key issue of national security. India must assume the leading role in this regulatory process, as many developing countries look towards it as a country without any bias towards either the US or the Sino-Russian cyber policy. As in the 2017 norm formulation process, the US and Russia proposed two resolutions that were passed by the UNGA First Committee on Disarmament and International Security at 73rd Session of the United Nations General Assembly, 2019). India voted for both of them, opening a new opportunity for proactively shaping norm formulation in keeping with the requirements and agendas of developing countries.

India's unbiased approach is deeply based on its constitutional values, in which individual rights are seen as a collective good. For example, when we talk about data protection, we refer not only to the protection of individuals' data but also to a system that would foster an environment for a free and fair digital economy. Unlike China, where the state sees itself above the individual, or US and European countries, where liberty is considered as freedom from state control and individuality is the focus of constitutional values, India sees the protection of personal data and the data economy as being complementary to each other, insofar as collective interest lies in individual interest. Therefore, India is fraying a way to protect individual rights while promoting the digital economy. As we saw, Free Basics sponsored by Facebook experienced a setback in India, checking the colonial approach of private US organizations.

Still, India should not further postpone its data regulatory framework. In a recent 2021 development, the mobile IP messaging application WhatsApp sought consent from users to share their data, including transaction data and location details, with Facebook, which means WhatsApp will share its users with Facebook, despite the latter being criticized for the Cambridge Analytica Scam. The Indian government sent 14 queries to WhatsApp and posted a note to protect Indian users from being exposed to greater security risks. Moreover, India banned 267 Chinese apps that have constantly mined Indian user data without proper consent and thus became a threat to national security as per reports received from the Indian Cyber Crime Coordination Center of the Ministry of Home Affairs. Thus, India has protected itself from data colonialism by private companies as well as vicious agendas hidden in state policies. India should not delay adopting a Personal Data Protection Act to protect its citizens from threats, as such companies thrive only in the context of lawlessness.

Cybersecurity and cyber laws are coupled to each other. To make a secure cyberspace, space laws and regulations should be framed in such a manner that any violator receives appropriate punishment. As cyberthreats are not exclusively internal but can come from any corner of the world, the IT Act of 2000 (amended in 2008) has largely become ineffective. The recent security breach at the Kundakulam Nuclear Power Plant has raised serious concerns, all the more so as it was not handled properly: the administration of the Nuclear Power Corporation of India Ltd. (NPCIL) initially denied the incident, and the North Korean hacker was not even traced [Madhavan N., 2019].

Most IT-related issues are covered by the Information Technology Act of 2008. However, despite its comprehensive nature, this act does not deal with all offenses or provide sufficient punishment for them. For example, section 66E of the act that concerns breaches of privacy stipulates only three years of punishment and a fine of two lakh rupees [Pathak U., 2017]. In addition, the act does not deal comprehensively with the ways of tackling international threats.

Hence, India should frame its cyber policies in a way that would allow it to trace and attribute cyberattacks. Many non-state actors such as tech companies and hackers are getting engaged in cyberspace architecture, and India must work to develop a cohesive approach to the regulation of cyberspace. As the Ministry of External Affairs (MEA) cannot deal with private organizations directly, India should push its private organizations to take part in the process.

Conclusion

The last national Cybersecurity Policy was adopted in 2013. It is high time to update it, as the world has greatly changed and is getting ready for a new digital revolution following the Covid-19 pandemic, with the cyberspace playing an increasing role in our daily life.

India should create a body with stakeholders from the Defense Ministry (DM) and the MEA, as both of these ministries have roles in cyber defense and cyber strategy. It should also involve security researchers and representatives of the private sector, civil society and the military to shape a better cyber strategy.

Just as regular military exercises take place with multiple countries, India should conduct cybersecurity exercises with different nations, especially developing countries when it could help in capacity building.

India's cybersecurity should become an essential part of its national security.

India should clearly define how international laws apply to cyberspace.

Though India already has a strong cybersecurity infrastructure, it should keep upgrading it as well as conducting hackathons to improve it.

India should promote the participation of the private sector in creating a safer cyberspace.

References

Appadurai A. (1991) Global ethnoscapes: Notes and queries for a transnational anthropology. In: R. Fox (ed.) Recapturing Anthropology. Santa Fe: School of American Research Press, pp.191–210.

Basu A., Hickok E., Rathi A., Trikanad S. (2018) Cyberspace and External Affairs: A Memorandum for India. Available at: https://cis-india.org/internet-governance/files/cyberspace-and-external-affairs (accessed: 14.02.2021)

Bhabha H. (1984) Of Mimicry and Man: The Ambivalence of Colonial Discourse. Available at: https://doi.org/10.2307/778467 (accessed: 04.06.2021)

Bhargava K. (2020) PM Modi's mantra for Atmanirbhar Bharat: Value-Addition to raw material, making finished goods. Available at: https://www.financialexpress.com/economy/pm-modis-mantra-for-atmanirbhar-bharat-value-addition-to-raw-material-making-finished-goods/2055739/ (accessed: 04.06.2021)

Brain J. (2021) The Cotton Industry. Historic UK. Available at: https://www.historic-uk.com/HistoryUK/HistoryofBritain/Cotton-Industry/ (accessed: 03.04.2021)

Brandom R. (2015) British "Karma Police" program carries out mass surveillance of the web. The Verge. Available at: https://www.theverge.com/2015/9/25/9397119/gchq-karma-police-web-surveillance (accessed: 07.02.2021)

Cheney-Lippold J. (2011) A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control. Available at: https://doi.org/10.1177/0263276411424420 (accessed: 04.06.2021)

Cohen J. (2007) Cyberspace As/And Space. Available at: https://scholarship.law.georgetown.edu/facpub/807 (accessed: 04.06.2021)

Cyberspace as Global Commons: The Challenges. (2012) DATAQUEST., Available at: https://www.dqindia.com/cyberspace-global-commons-the-challenges-1/ (accessed: 04.03.2021)

Dijck J. van (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, no 2, pp. 197–208. Available at: https://doi.org/10.24908/ss.v12i2.4776 (accessed: 10.05.2021)

Dijck J. van, Poell T., Waal M. de (2018) The Platform Society. Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190889760.001.0001/oso-9780190889760 (accessed: 04.06.2021)

Ghosh S. & Kanter J. (2019) Google says data is more like sunlight than oil, just 1 day after being fined $57 million over its privacy and consent practices. Available at: https://www.businessinsider.in/google-says-data-is-more-like-sunlight-than-oil-just-1-day-after-being-fined-57-million-over-its-privacy-and-consent-practices/articleshow/67640224.cms (accessed: 4.06.2021)

Gitelman L. (2013) *"Raw data" is an oxymoron*. Cambridge: MIT Press, 192 p.

Haupt M. (2016) Data is the New Oil—A Ludicrous Proposition. Medium. Available at: https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294 (accessed: 26.02.2021)

Hauser-Schäublin K., Dickhardt M. (2003) Kulturelle Räume—Räumliche Kultur. Available at: https://www.lit-verlag.de/isbn/978-3-8258-6799-4 (accessed: 20.08.2020)

Hiranandani G. (2000) *Transition to Triumph: History of the Indian Navy, 1965–1975*. New Delhi: Spantech & Lancer. 415 p.

Ho W.-C. (2008).The Transcendence and Non-Discursivity of the Life world. *Springer Science + Business Media,* no 3, pp. 323–342.

Jasanoff S. (2004). Ordering knowledge, ordering society. In: States of Knowledge: The Co-production of Science and the Social Order. Available at: https://www.routledge.com/States-of-Knowledge-The-Co-production-of-Science-and-the-Social-Order/Jasanoff/p/book/9780415403290 (accessed: 04.06.2021)

Kokot W. (2007) Culture and Space — anthropological approaches. *Ethnoscripts* , no 9, pp. 10–23.

Kumar A. (2014) Norm Entrepreneur, Catalyst or Challenger? India in the Nuclear Non-proliferation Narrative. Available at: https://journals.sagepub.com/doi/abs/10.1177/0971523115592493 (accessed: 03.04.2021)

Latour B. (1987) Science in Action. Available at: https://www.hup.harvard.edu/catalog.php?isbn=9780674792913 (accessed: 04.06.2021)

Lindsay J. (2015) The Impact of China on Cybersecurity: Fiction and Friction. Available at: https://www.belfercenter.org/publication/impact-china-cybersecurity-fiction-and-friction (accessed: 04.06.2021)

Madhavan N. (2019) Is India cyber security ready? Available at: https://www.thehindubusinessline.com/opinion/columns/is-india-cyber-security-ready/article29911679.ece (accessed: 04.06.2021)

Mishra D., Chanchani M. (2020) Internet users in India: For the first time, India has more rural net users than urban. Available at: https://timesofindia.indiatimes.com/business/india-business/for-the-first-time-india-has-more-rural-net-users-than-urban/articleshow/75566025.cms (accessed: 04.06.2021)

Mozur P. (2015) New Rules in China Upset Western Tech Companies. Available at: https://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html (accessed: 04.12.2021)

Roser M. (2018) The Internet's history has just begun. Available at: https://ourworldindata.org/internet (accessed: 4.06.2021)

Pathak U. (2017) Cyber security and cyber laws in India: focus areas and issue areas. Vol. 6, issue 1. DOI: 10.5958/2277-937X.2017.00008.9

Preeti (2016) Colonial codification of education in India until 1920. *Journal of Indian Education,* no 2, pp. 29–44.

Rao P. (2015) *From Fishing Hamlet to Red Planet: India's Space Journey.* Bengaluru: ISRO, 736 p.

Xi Jinping P.E. (2015) Remarks. Available at: https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (accessed: 03.02.2021)

Said E. (2003) *Orientalism*. London: Penguin, pp. 1–28, 350–353.

Scholz L. (2018) Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies. Tennessee Law Review, vol. 85, p. 2020. DOI: 10.2139/ssrn.3252543

Segal A. (2016) China, Encryption Policy, and International Influence. Hoover Institution. Series Paper No. 1610. Available at: https://www.lawfareblog.com/china-encryption-policy-and-international-influence (accessed: 02.03.2021)

Segal A. (2020) China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. *NBR Special Report,* no 87, pp. 85–100.

Sherman J. (2019) How Much Cyber Sovereignty is Too Much Cyber Sovereignty? Available at: https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty (accessed: 07.12.2021)

Singh S. (2013) Govt. Violates privacy safeguards to secretly monitor Internet traffic. Available at: https://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internet-traffic/article5107682.ece (accessed: 04.03.2021)

Thengadi D. (1998) *The third way*. Bengaluru: Sahitya Sindhu Prakashana, 283 p.

Venables A. (2019) Establishing Cyber Sovereignty — Russia Follows China's Example. Available at: https://icds.ee/en/establishing-cyber-sovereignty-russia-follows-chinas-example/ (accessed: 16.12.2020)

Young R. (1995) Foucault on Race and Colonialism, Available at: https://www.semanticscholar.org/paper/Foucault-on-Race-and-Colonialism-Young/b4677c88a97256945644050fb7b2a33b1700503a (accessed: 04.06.2021)