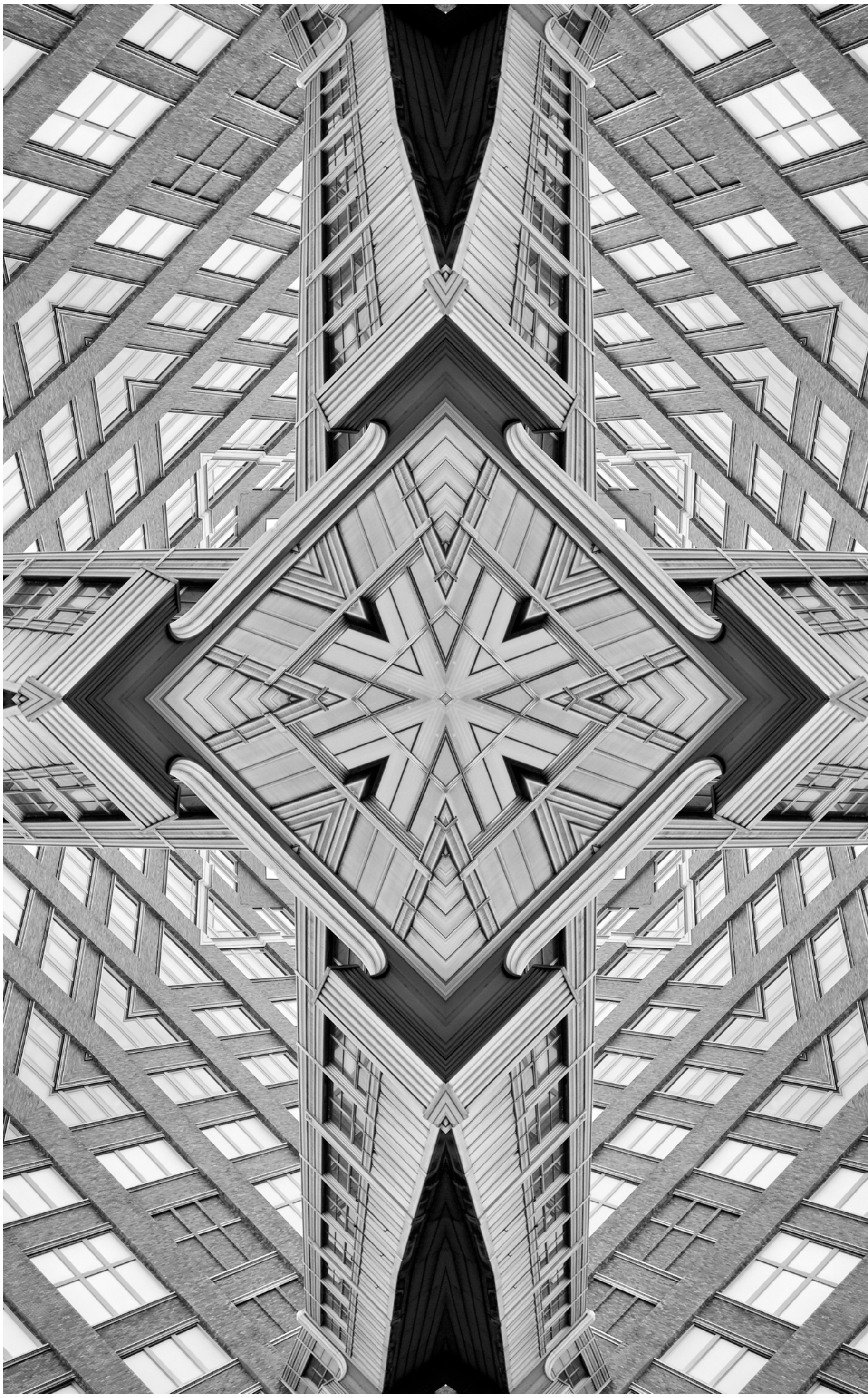
Issue Brief

ISSUE NO. 602
DECEMBER 2022

OBSERVER
RESEARCH
FOUNDATION



Cyber Sovereignty: In Search of Definitions, Exploring Implications

Madhuvanthi Palaniappan

Abstract

The increasing dependence on the internet across the spectrum is pushing some states to adopt measures to exert their sovereignty over cyberspace. Certain global events have also acted as a catalyst for states to pursue cyber sovereignty. The involvement of multiple stakeholders and the borderless character of the virtual world have made sovereignty a complex affair in this domain. This brief seeks to illuminate the concept of 'cyber sovereignty' and the implications of its pursuit, including the fragmentation of the internet and the violation of people's fundamental rights.

Attribution: Madhuvanthi Palaniappan, "Cyber Sovereignty: In Search of Definitions, Exploring Implications," *ORF Issue Brief No. 602*, December 2022, Observer Research Foundation.

Introduction

Technological advancements have made cyberspace an integral part of human lives. An enormous amount of data is generated using cyber applications; governments and private enterprises process this data to obtain actionable intelligence, which aids them in achieving specific objectives. A state's desire to control 'cyberspace' within its borders is achieved by exercising what is called 'cyber sovereignty'. While some countries such as the United States (US) support the free flow of information, others like China, by default, restrict the flow for its citizens, leading to the fragmentation of the internet.

Cyberspace, in its entirety, has been created by humans; unlike other realms that are more static, it continues to expand. This fundamental characteristic makes it difficult to define what comprises 'sovereignty' over the domain. Multiple stakeholders have been involved in its creation since its inception, including governments, the private sector, and civil society. In contrast to other technologies whose development is driven by policy, here it is technology which drives policy decisions. These characteristics make cyberspace governance complex and lead to confrontations among states and other stakeholders. Such face-offs have led to the rise of virtual borders in cyberspace. Cyber sovereignty, and its perception by global powers, requires closer assessment.

This brief explores the ambiguity involved in the concept of 'cyber sovereignty' and its applications. It probes how cyber sovereignty as a concept has transformed with the emergence of both opportunities and threats in cyberspace. It underlines the incidents that have acted as catalyst for states to exercise cyber sovereignty, and explores the implications.

The Emergence of Cyber Sovereignty

It is often said that "information is wealth."[1] Competition has developed between states, and between state and non-state actors, to control and access this wealth. Since most of the development of both hardware and software initially took place in the West, particularly in the United States, the West had a monopoly over this technology and ruled the industry and until recently, there was little or no restriction on the free flow of information on the internet. A crucial shift has happened in the past few years.

Cyber security expert Daniel Kuehl defines cyberspace as "a global domain within the information system whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via independent and interconnected networks using information-communication technologies."[2] Traditionally, cyberspace was understood only in three layers: the physical/hardware, neural/software, and data. Alexander Klimburg, in his book *The Darkening Web*, introduced a fourth layer that deals with the social interaction among the three layers: "If cyberspace can be said to have a soul or mind, this is where it is." Establishing control over all the layers is necessary to build sovereignty in cyberspace.[3]

Control over these layers is established by building a virtual frontier that helps states to exercise their sovereignty. When the number of users expanded worldwide and the potential military, political and economic benefits of the internet became more apparent to states, they started to exercise control over it within their borders using political, economic, cultural, and technological channels. The vulnerabilities of cyberspace have been exploited to achieve political goals, either by employing malicious code like Stuxnet[a] or gathering intelligence in the case of the PRISM[b] programme, or mobilising anti-government protests during the Arab Spring.[c] Such developments led some states to adopt policies and technologies that will enable them to exercise control over cyberspace.

In 1996, US poet and political activist John Perry Barlow affirmed the independence of cyberspace, writing, "Cyberspace does not lie within … borders."[4] He considered cyberspace distinct from other spaces, where states had no role. He believed cyberspace could bring the global community together,

[a] Stuxnet is a malicious worm said to have caused much damage to Iran's nuclear programme by targeting Supervisory Controls and Data Acquisition (SCADA) systems.

[b] PRISM is a program under the National Security Agency of the US that gathered communication information from the US-based internet companies.

[c] The anti-government protests that erupted in several countries of West Asia and North Africa in the early 2010s.

The Emergence of Cyber Sovereignty

being everywhere and nowhere at the same time, and providing a platform for expression without restriction across national boundaries irrespective of state ideology or political organisation. Recent events tend to prove these notions wrong.

If the Australian scholar Headly Bull's concept of international order is applied in cyberspace, then it is necessary for states to exert sovereignty over cyberspace for establishing an international cyber order.[5] This helps understand why states have restricted the free flow of information in the last few years. In particular, though China and Russia accepted such free flow initially, their governments quickly realised that this could negatively affect them. They opposed the internet's open design and tried to impose sovereignty in cyberspace.

The concept of sovereignty and the modern state goes back to the end of the 30-year war of the 17th century, when countries agreed to have sovereign rights over their territories and domestic affairs, limiting other states' interference. Russia and China have extended the sovereignty concept to justify controlling and filtering the information that crosses their borders.[6] Sovereignty has always remained contested and ambiguous; states have used this ambiguity to interpret and propagate the meaning that suits their interests. According to the *Tallinn Manual on International Law Applicable to Cyber-warfare*, 'sovereignty' means 'territoriality'—prohibition of intervention or use of force or armed attack—that triggers the right of both individual and collective self-defence. Earlier, sovereignty meant a set of rules; in recent times, it has developed into a principle and has grown into a premise by itself from which the rules emerge.

Here arises the crucial question of whether states should be held accountable for cyber-attacks emanating from their territory, since it comes under the state's sovereignty. The International Court of Justice (ICJ) defines sovereignty as that which "confers rights upon states and imposes obligations on them."[7] This implies that states must control their cyber infrastructure and prevent it from being knowingly or unknowingly used to harm other states and non-state actors. Therefore, the state, or the citizens of the state, if involved in attacking other states or non-state actors' cyber facilities, also come under the ambit of cyber sovereignty.[8]

The Emergence of Cyber Sovereignty

Unlike other spaces such as land, sea, air, and outer space, cyberspace was created by humans; therefore, complete control can be established over it. Countries have tried to frame policies and rules to regulate cyberspace by building the necessary infrastructure. This can be seen as either a defensive mechanism that states use to protect their own critical infrastructure or a framework adopted to exploit other states' resources. It has led to a security dilemma and added fuel to the fire of great-power politics. Realising its importance, states have started to see cyberspace as equivalent to physical territory, and are building virtual walls to protect their 'cyber territory' with the help of various technologies.

Security vulnerabilities in cyberspace are one of the main reasons for this drastic change. These vulnerabilities continue to be exploited today. Cyber-attacks and social media-led anti-government protests prompted many states to rethink the open use of the internet.

Table 1 summarises the key global events that prompted states to pursue cyber sovereignty.

Table 1: Global Events in Cyberspace and Consequences

Global Events	Consequences
2007 – Coordinated cyber-attacks on websites of Estonian organisations and institutions. They occurred amidst a conflict between Russia and Estonia over the relocation of a bronze soldier in Tallinn, about which Estonians and Russians have very different historical perceptions.	Estonia relocated its physical cyber infrastructure to an undisclosed location in Luxembourg under the jurisdiction of Estonia to protect its data in case of a future military attack, further complicating sovereignty issues in cyberspace.
2008 - Operation Buckshot Yankee was a malicious attack that targeted US military systems. It is considered one of the worst cyber security breaches in the history of the US military.	The United States Cyber Command was created to strengthen the US Department of Defence capabilities.

2010 – Stuxnet attack on Iran's nuclear facilities at Natanz	Iran adopted multiple policies to strengthen its cyberspace. It is following China in its pursuit of cyber sovereignty. The attack made states realise the vital importance of cyber security and its integration with national security. It set off a worldwide discourse on cyberspace governance.
2013 – Edward Snowden's disclosure about the PRISM programme of the US	It acted as a catalyst in promoting the idea of cyberspace as a sovereign territory, leading states to adopt data sovereignty and localisation measures. With the General Data Protection Regulation (GDPR) being implemented by the European Union in 2018, many other countries have adopted similar policies.

Source: Author's own, using various open sources.

Cyber power is vital in the 21st century, being the fifth arena where wars can be fought, after land, air, water, and outer space. A state-launched cyber-attack is a demonstration of the cyber capabilities of the attacker. It can have detrimental effects on the adversary's critical infrastructure, such as telecommunications, transport, defence, energy, and banking. Therefore, there is competition among nations to have advanced cyber capabilities; such power plays a role in global power politics. Unlike in the case of the other four dimensions of warfare, in cyberspace, even relatively small states with limited resources, such as North Korea for instance, can pose a considerable threat. Any state attacked also improves its cyber infrastructure by bringing in new frameworks and policies to protect its critical infrastructure, so as to ensure its sovereignty in cyberspace.

During the Arab Spring, protesters extensively used social media, which made world leaders realise how the internet can empower people to challenge established governance systems. The Arab Spring, followed by Stuxnet and the Edward Snowden leaks, provoked fear that the US was exploiting cyberspace to pursue its geostrategic goals. Russian President Vladimir Putin called the Internet "a CIA project", and adopted various data localisation policies to protect Russian data.[9] These, in turn, raised fears of the global internet breaking up, also referred to as "balkanisation of the internet" or "internet fragmentation". Balkanisation of the internet would endanger global internet connectivity by limiting free flow of information—a pillar of the internet.

The Stakes of Global Powers

During the Cold War, the US invested in developing the Advanced Research Project Agency Network (ARPANET), a forerunner of the internet. The then Union of Soviet Socialist Republics (USSR) also tried to develop an information network to establish complete control over its industries. Norbert Weiner's work, *Cybernetics, or Control and Communication in the Animal and the Machine* published in 1948, inspired the USSR to work on OGAS in the early 1960s, the Soviet version of ARPANET. Some analysts claim OGAS was an extension of the surveillance system of the USSR, instituted by its main security agency, the KGB. Though it made some initial progress, it was eventually a failure, largely due to financial constraints and political reasons.

John Postal and Tim Berners-Lee, while developing the Domain Name System (DNS) and the World Wide Web, respectively, would never have thought their discoveries could lead to the revolution the internet has become. Though the US government funded and pushed for the development of the internet, it was created mainly by a community of scientists. Its usage did not remain restricted to the West but soon became a global phenomenon. In his book, *How Not to Network a Nation,* Benjamin Peters notes: "The capitalists [the US] behaved like socialists, and the socialists [the USSR] behaved like capitalists."[10] In recent years, however, China appears to have realised the Soviet dream, establishing complete control over its infrastructure.

With the increase in internet usage, the US monopoly of control over root servers alarmed Russia and many other states. In 1998, Russia initiated a discussion in the United Nations General Assembly with a draft resolution titled "Developments in the field of information and telecommunications in the context of international security", highlighting its concern over cyber technologies being used by state militaries and terrorists alike.[11] Subsequently, a Group of Governmental Experts was formed to deal with cyber security-related issues, in which Russia, and in recent years China, have participated actively, mainly to oppose US domination.

The US monopoly continued into the first decade of the 21st century. Much has changed since. The Russia-led coalition challenged the practice of internet governance dominated by the US, and eventually, due to increasing international pressure, in 2016, the US transferred the functions of the Internet

Assigned Numbers Authority (IANA) to the Internet Corporation for Assigned Names and Numbers (ICANN), a multistakeholder non-profit organisation.[12] China and Russia considered the IANA function being controlled by the US a violation of their sovereignty; in all, 89 countries, including Russia, China, and Iran, opposed the US domination. To further strengthen control over their own cyberspace, most countries have adopted cyber laws and rules to prevent external interference and protect their sovereignty. China has effectively established control over its primary infrastructure, the middle layer (software), and its data using what has been called the 'Great Firewall of China', which monitors its citizens' activity in cyberspace with the help of private players.

The Great Firewall of China uses techniques such as internet protocol (IP) blocking, DNS 'poisoning',[d] self-censorship, and manual enforcement. The government and app owners employ thousands to monitor the content being shared by users. The monitoring is so advanced that messages offensive to the government are blocked before they can go viral. Restrictions are often placed on posting content related to specific issues. Google is a widely used search engine across the world, which, along with other applications and with the help of the data it generates, can profile every user. China has thus banned Google, along with other Western multinational corporation-owned applications such as Twitter, Facebook, and WhatsApp, providing its citizens its own versions such as the 'Baidu' search engine and 'WeChat' messaging. Though it has many privately owned companies such as online retailer Alibaba and entertainment and video gaming giant Tencent, the Communist Party of China has effective control over them.

China justifies its control by claiming that the West uses cyberspace as a tool for the surveillance of the Chinese population. It also fears that the ideological and political threat from the West could create instability and threaten its security. Another justification offered is the possibility of competing nations exploiting the large amount of data its citizens generate.

[d] Domain Name System DNS poisoning is a hacking technique tha that reroutes traffic from the actual website to a malicious website by taking advantage of the vulnerabilities within the DNS.

The Stakes of Global Powers

Similarly, Russia has 'Mail.ru' (the equivalent of Gmail) and the search engine 'Yandex'. It has introduced oversight mechanisms to regulate the private telecommunications sector. It is also working on creating its own internet infrastructure called 'Runet', which gives the government more power over its citizens. Its sovereign internet law came into force in 2019, disconnecting Russia's internet from the rest of the world. It has justified the action as a national security measure to protect its cyberspace.[13] Some other states are also developing a closed form of the internet by including content filters and block lists.[14]

Western powers such as the US, France, and the UK too, have their data protection laws, but they do not restrict the free flow of information except by limiting certain sensitive content like child pornography. In recent years, social media platforms such as Facebook and Twitter have been used to spread false propaganda and influence citizens during elections, posing a considerable challenge to the more liberal states.[15]

> "In the late 2010s, many countries started adopting cyber laws and rules to prevent external interference and protect their sovereignty."

Implications of Cyber Sovereignty

Cyber sovereignty has various implications, from the fragmentation of the internet to violation of human rights.

The internet was created to promote the free flow of information, but cyber sovereignty works the other way around. Restricting the flow of information can also put global businesses at risk due to the lack of interoperability it leads to. At the same time, inventions and innovations in various technologies such as artificial intelligence, telecommunications, big data, the internet of things, and cloud computing are increasing the importance of data; protecting critical infrastructure becomes part of the national security agenda. This infrastructure enables health systems, logistics, industries, transportation, education, and information technology. It provides access to all the data, and in the absence of protection, some states will be able to exploit the vulnerability of others, compromising their sovereignty.

Control over such data could lead to new forms of colonialism and imperialism, commonly referred to as 'data colonisation' and 'data imperialism' in the digital era. States and private players can overreach their powers and violate human rights through cyberspace surveillance, controlling information flow, and enforcing internet shutdowns. The implications are broad, impinging on citizens' rights such as privacy, freedom of expression, access to information, press freedom, freedom of belief, non-discrimination and equality, freedom of assembly, freedom of association, due process and personal security.[16] For instance, access to geolocation data can give insights into people who participated in a protest. Further, based on a user's online behaviour, it is possible to determine a person's sexual orientation, political affiliation and religious beliefs.

In 2009, seeking justice for their co-workers whom the Han Chinese killed in a doll factory, Uighurs, a Muslim minority community in China, organised a protest using Facebook and Uighur-language blogs. Following this incident, Facebook and Twitter were blocked across the country, and the internet was shut down for ten months in the region.[17] Following the incident, the Chinese government, with the help of the private sector, developed AI-enabled applications like the Integrated Joint Operations Platform (Ijop) to monitor the daily activities of Uighur Muslims. This app obtains information like skin colour, facial features, properties owned, payments, and personal relationships, and reports if there are any suspicious activities. An investigation is initiated if the systems flag any person. Data is gathered 24/7 to carry out mass surveillance.[18]

Conclusion

The cyber domain will become even more critical and integral to human life in the coming years. However, the ambiguity in defining what constitutes 'sovereignty' will remain a significant challenge, even as countries adopt protective measures for their own territories. Compounding the challenge is that states have different perspectives on the free flow of information.

The dichotomy of states trying to protect the data generated in their territory by introducing data protection laws but, simultaneously, wanting to exploit other states' data is adding to the complexity. It is one of the main reasons countries cannot reach a consensus on cyber-related matters. The West continues to promote the open internet, whereas countries like China and Russia support the closed model. This has resulted in implications such as the fragmentation of the internet and the violation of people's fundamental rights.

Madhuvanthi Palaniappan *is a Research Assistant at the Council for Strategic and Defence Research, Delhi. She has a Master's degree in Geopolitics and International Relations.*

Endnotes

1. Herbert A Simon, "Designing Organizations for an Information-Rich World," *Computers, Communications, and the Public Interest* (1971): 37 – 72.

2. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 38.

3. Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (Penguin, 2018), pp 29.

4. John Perry Barlow, "Electronic Frontier Foundation," *A Declaration of the Independence of Cyberspace* 56, no. 3 (1996) https://www.eff.org/cyberspace-independence

5. Andrew Liaropolous, "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?," *Journal of Information Warfare 12*, no. 2 (2013): 19–26.

6. Chris C Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (2011): 32-61.

7. Michael N Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

8. Eric Talbot Jensen, "Cyber Sovereignty: The Way Ahead," *Tex. Int'l LJ* 50 (2015): 277.

9. Ewen MacAskill, "Putin Calls Internet a 'CIA project' Renewing Fears of Web Breakup," *The Guardian*, April 24, 2014, https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia

10. Chris Baraniuk, "Why the Forgotten Soviet Internet Was Doomed From the Start," *BBC Future*, October 26, 2016, https://www.bbc.com/future/article/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start

11. United Nations General Assembly, "Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly," *United Nations Digital Library*, April 04, 1998, https://digitallibrary.un.org/record/265311?ln=en

12. ICANN, "Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends," *ICANN*, October 01, 2016, https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en

13. Elizabeth Schule, "Russia just brought in a law to try to disconnect its internet from the rest of the world," *CNBC*, November 01, 2019, https://www.cnbc.com/2019/11/01/russia-controversial-sovereign-internet-law-goes-into-force.html

Endnotes

14. Internet Society, "Internet Society Perspectives on Internet Content Blocking: An Overview," *Internet Society*, March 24, 2017, https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

15. Bolane Olaniran and Indi Williams, "Social Media Effects: Hijacking Democracy and Civility in Civic Engagement," in *Platforms, Protests, and the Challenge of Networked Democracy*, February 27, 2020, doi:10.1007/978-3-030-36525-7_5, pp: 77–94

16. Adrian Shahbaz et al., "Special report 2020: User Privacy or Cyber Sovereignty?," *Freedom House, July 2020,* https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

17. Darren Byler, "China's Hi-Tech War on its Muslim Minority," *The Guardian,* April 11, 2019, https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition

18. Human Rights Watch, "China's Algorithms of Repression," *HRW*, May 1, 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org