Critically analyse the concept of "(digital) sovereignty" with examples from different countries that illustrate its relevance or not.

Introduction:

The invention of the Internet in the 1980s was hailed as the technological advancement that was to be the unifying force that transcended national borders, reduced hurdles in international communication and brought the world together. However, with increased data sharing across borders, more global data networks and technological multinational corporations, the concept of 'digital sovereignty' has made a comeback in mainstream international politics. States are now demonstrating a renewed passion for reestablishing their 'sovereignty' over the digital.

This essay will analyse 'digital sovereignty' by using relevant literature and examples. It will first discuss the notion of sovereignty and theories defining the significance of states in international relations. Next, the essay will explore how sovereignty relates to the digital. Lastly, we will see whether the idea of 'digital sovereignty' holds relevance in the modern world.

What is Sovereignty? Do states matter in international relations?

Conceptualising 'digital sovereignty' and analysing its relevance, must be preceded by a strong understanding of what the notion of 'sovereignty' implies even when not relating to the digital.

Sovereignty is a concept that refers to the absolute control that a state exercises within its own territory. Often, this control is tied to the political authority that governs a nation. Daniel Philpott, in his entry on sovereignty in The Stanford Encyclopedia of Philosophy, states that "The modern polity is known as the state, and the fundamental characteristic of authority within it, sovereignty," defining it as the "supreme authority within a territory," (Philpott, 2003).

He goes on to further make a case for Sovereignty: its holder must have supreme authority over a territory, derived from a legitimate source such as a constitution (modern governments), God (theocracy) or a hereditary law (monarchy/dictatorship) (Philpott, 2003). Two major movements have played a role in perpetuating the modern understanding of a sovereign state.

The first is the Treaty of Westphalia, signed on October 24, 1648, as a resolution to the Thirty Years' War and the Eighty Years' War. The latter was a Dutch war of Independence, while the former was a series of conflicts between Catholic and Protestant states looking to assert dominance. The Westphalian treaty was central to the resolution of the conflict, for it allowed Christian non-denominations to continue to practice their faith, but most importantly, it acknowledged "that each state has sovereignty over its territory and domestic affairs, to the exclusion of all external powers, on the principle of non-interference in another country's domestic affairs," (Lumen Learning, n.d.).

The second of these movements is the 'Theory of Realism', which developed after the Second World War, by philosophers such as E.H Carr and Hans Morgenthau. Primarily a product of the Cold War, the theory had quasi-Marxist origins. According to E.H Carr, the real conflict in international relations was to be found in between the 'haves' and the 'have nots' (Brown & Ainley, 2005).

The realist school believed that states were governed by the same laws as people – all policies thus, were introduced with power at the center. This is reflected in Morgenthau's following statements "All politics, domestic and international, reveals three basic patterns; that is; all political phenomena can be reduced to three basic types. A political policy seeks either to keep power, increase power or to demonstrate power," (Morgenthau, 1960, cited in (Archer, 2001, pp. 119-120)). Thus, the primary aim of all states is survival, corresponding to the three

aims of political power – policy of the status quo (keeping power), imperialism (increasing power), and policy of prestige (demonstrating power) (Archer, 2001). This keeps the decision-making power in the hands of the statesmen.

In terms of where international non-governmental organisations (INGOs) fit into the context, Morgenthau acknowledged their role, while continuing to assert that states had all the power.

Although the theory clarifies the state of world politics during the Cold War, it is not perfect and is open to criticism. The first of these issues is the lack of any real challenge to the status quo – rather than try and understand the changing dynamics, the realist school of thought simply accepts modern day international politics as dependent solely on states and does not consider the role of international organisations (Archer, 2001). The theory also neglects the importance of economics, technical advancements, and culture in favour of maintaining peace.

Thus, the main problem with the realist school is its preoccupation with the state as the center of power: interstate relations matter most, and the state can and will regulate should it want to (Brown & Ainley, 2005, p. 35).

This is where the 'Theory of Interdependence' comes in. Proposed by thinkers such as Robert Keohane and Joseph Nye, the theory tries to circumvent the above stated issues. First it disregards the assumption that 'interstate relations matter most' – states are neither the only actors, nor are they unitary, other actors such as international organisations, civil society and even crime syndicates play a role in international relations (Brown & Ainley, 2005). The theory of "complex interdependence" differs from the theory of realism in three main ways. It assumes that there exist "multiple channels of access between societies," force holds little power in most international relationships, and "there is no hierarchy of issues," (Keohane and Nye, 1997/2000, cited in (Brown & Ainley, 2005)).

The theory acknowledges that various actors such as civil society groups, social movements, and businesses amongst others, have a part in the international decision-making process, and that there are other issues in international politics such as the climate change, trade, crimes, etc., are also important and are not necessarily linked to one another.

Both the theories assign a certain importance to the state – the realist theory offers complete control to the state, while interdependence suggests that the state does have powers, albeit they are shared with other stakeholders that can exert control in the decision and policy making processes. An example of the realist theory in action is the establishment of the Great Firewall of China (discussed in detail below). The Chinese Internet Policy is governed only by the State – no other stakeholders play any part in the creation of this policy. On the other hand, we have the example of India – Net Neutrality in India was enforced through the participation of various actors like civil society organisations, technology conglomerates, and non-governmental regulatory authorities. A Consultation paper seeking comment was released and everyone was invited to comment, before the regulatory authority ruled in favour of Net Neutrality and the government enacted their suggestions (Soni, 2015).

Types of Sovereignty: Where does Digital fit in all this?

Sovereignty, therefore, has been historically understood as the absolute authority a state exercises over the citizens, resources, and developments within its territory. However, sovereignty can be understood in more contexts than just the historical. When understood as the existence of an independent state without undue pressure and external influence (as asserted by the Treaty of Westphalia), sovereignty becomes the basis for international law. It can also mean the autonomy and the right to self-determination in other cases (Internet Society, 2022).

So, how does the Digital come into the picture?

Digital Sovereignty, in the simplest of terms can be taken to be mean sovereignty as it relates to the digital. This involves the technology that creates the digital, the data that is generated from the digital, the data that is shared using the digital and the products made available as a result of the digital. Thus, Digital Sovereignty can then be defined as "the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create," (Fleming, 2021).

Although it has historically been associated with autocratic and authoritative regimes (Couture & Toupin, 2019, p. 2310), today, digital sovereignty is at the center of internet policies across the globe.

Much like the concept it is based on, digital sovereignty is treated as an umbrella term while referring to the various sovereignties related to the digital.

The first of these emerged in the United States from the technological advancements in the 1970s. The concept of technological sovereignty emerged from debates related to these advancements. It was defined by the Science Council of Canada as a means "to develop and control the technological capability to support national sovereignty," (Globerman, 1978: 43, as cited by (Couture & Toupin, 2019)). Technological sovereignty referred to the freedom of developing technologies to boost growth in all sectors.

As with the theory of realism, this version of sovereignty, too, was designed to give the state the power in the realm of international relations – technological sovereignty meant having the ability to become technologically advanced for the benefit of the state.

Another version of digital sovereignty, which developed in the mid-1990s and has still held strong in certain ways, is Cyberspace sovereignty. This idea hinges upon the notion that the Cyberspace as a domain within the network environment is free from the ubiquitous sovereignty of the physical and territorial state. Shared first by John Perry Barlow in his 1996

A Declaration of the Independence of Cyberspace, the idea was aimed at disregarding state sovereignty in response to states asserting their sovereignty on that which had not emerged from their regulations (Couture & Toupin, 2019).

Cyberspace sovereignty remains a popular theory even today, albeit with tweaks. Since, the internet is 'transnational' and allows for the sharing of data indiscriminately across borders, this makes it beyond state control and therefore independent of state sovereignty. Timothy S. Wu pointed out that not only was it possible to regulate the cyberspace, but it was possible to do so on several fronts. The most important of which was by regulating hardware (Wu, 1997, p. 651) – "By exercising control over the physical components required for Internet access, the state can regulate cyberspace."

Wu also states that it is possible to regulate the cyberspace through software and activities on the internet. Software regulation, he says, is most effective at the router level and the end user level. The router level makes use of a firewall, while the end-user level makes use of "end-user filtering software," to filter out content (Wu, 1997). While the presence of the 'free internet' across most sections of the world might be able to support the cyberspace as a sovereign as imagined by John Perry Barlow, Wu's hypotheses is supported by the presence of the 'Great Cannon of China.'

Before I elaborate on China's example, I would like to talk about another aspect of sovereignty that is associated with Digital Sovereignty. This is the concept of Personal Digital Sovereignty. As the name suggests, it relates to the authority that individuals have over the 'digital' that they interact with or create. This can include the data that they share or create, the technology (software and hardware) that they use, and even the content they might access. Tied to this is Data Sovereignty – which refers specifically to the authority individuals or nation

states have over the data that is generated, owned, or shared by the former, or the latter's citizens.

Coming back to the Chinese example, China has always censored the cyberspace and restricted access to it at some level.

Before 2015, the Chinese internet was censored using something known as the "Great Firewall of China." The West's version of the Internet is perpetuated in the country as going against Chinese values. Fang Binxing invented the "Golden Shield" which "enabled the government to inspect any data being received or sent, and to block destination IP addresses and domain names," (Economy, 2018). Later legislation ensured that companies that provided Internet services followed a set of rules and that certain content remained restricted.

The Golden Shield Project, as it is officially called, makes use of techniques such as "IP blocking, which denies the IP addresses of specific domains, packet filtering, which scans packets of data for controversial keywords, credit records, and speech and facial recognition," (Stanford, n.d.).

Despite this, the Chinese were able to access relative freedom on the internet: "Chinese citizens used virtual private networks (VPNs) to access blocked websites. Citizens banded together online to hold authorities accountable for their actions, through virtual petitions and organising physical protests," (Economy, 2018).

However, with the coming of Xi, "Within the virtual world, as in the real world, the party moved to silence dissenting voices, to mobilise party members in support of its values, and to prevent foreign ideas from seeping into Chinese political and social life," (Economy, 2018). In 2015, researchers, led by Bill Marczak, noticed the newest in Chinese censorship tools – the Great Cannon of China.

Their report states that “The Great Cannon is not simply an extension of the Great Firewall, but a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can arbitrarily replace unencrypted content as a man-in-the-middle,” (Marczak, et al., 2015). This means that the tool can “rewrite the internet on the fly,” (Hern, 2015).

This example supports Wu’s claims that any state wishing to regulate the cyberspace can do so using software regulation at both the router and the end-user level.

The Relevance of Digital Sovereignty:

But what does this mean for digital sovereignty in the modern world? Does it have any relevance in modern international relations and politics?

The Chinese example illustrates that despite the various ways that digital sovereignty can be understood – technological, personal, data, and cyberspace – states continue to take digital sovereignty seriously. Let us continue with the Chinese example to understand this statement.

The technological aspect of digital sovereignty can be viewed in the Chinese example through their insistence on making use of indigenous webservices rather than those innovated by America – Google, Yahoo and Facebook have been banned in the country for the past two decades, instead the Chinese make use of indigenous services such as Baidu, Weibo, and Douyin as substitutes. The very existence of the Great Chinese Firewall, as pointed out earlier, is proof of the Chinese state exerting their sovereignty over the cyberspace. By blocking most international data flows – either through the Firewall or the new Great Canon, Chine ensures that they are also maintaining sovereignty over the data of their citizens (The Economist, 2020).

According to a report by the Internet Society, it is possible to highlight two approaches to Digital Sovereignty: “a) Policies that assert national security through greater state control;

and b) policies that seek economic self-determination driven by economic actors," (Internet Society, 2022).

Countries like China, Russia, Australia, and Vietnam fall under the first category. As is depicted by the Chinese example, these policies are aimed at fortifying the nation's sovereignty by demonstrating the extent of its regulation on the digital.

In Russia, for example, the Internet did not face any serious regulation until the 2010s, since when, "Russian authorities are actively pursuing a digital sovereignty strategy that focuses on an autonomization of the RuNet through a complex dialectic of law and infrastructure-based enforcement, aimed at countering foreign 'influences' and agents, as well as their devices and applications; in the process, Russian authorities are attempting to remove their citizenry, as much as possible, from the contingencies and dependencies of a hyperconnected world," (Musiani, 2022).

On the other side of the coin, are examples of countries like India, the EU, and Rwanda. The focus here is on technological sovereignty, i.e., on reducing the reliance on foreign technology. An example is India's Data Centre Policy, 2020, which is aimed at "meeting the data security needs in the country," along with bring improvements and enhancing growth in the domestic sector, facilitating standardisation and "promoting sector competitiveness through various fiscal and non-fiscal incentives," (Ministry of Electronics & Information Technology, 2020). This policy can also be seen as a data protectionist approach, with the aim of empowering the Indian state to handle the data of its own citizens, as the EU aims to do with the General Data Protection Regulation.

Conclusions:

Sovereignty and the digital are two concepts that hold a lot of significance in today's world and are yet are hard to define clearly. This article has critically analysed the notion of

sovereignty from the historical lens, along with the examination of the various theories of international relations to understand its importance and the nature of modern sovereign states. The article then uses this knowledge to scrutinize the digital sovereign and analyse whether it holds any relevance in modern politics. Using examples from countries like China, Russia, and India, I have tried to provide a complete picture of how digital sovereignty is relevant, because modern nation states us the digital as another space to assert their authority as sovereign states.

List of References

Archer, C., 2001. *International Organisations.* 3 ed. London: Routledge.

Brown, C. & Ainley, K., 2005. *Understanding International Relations.* 3 ed. New York: Palgrave Macmillan.

Couture, S. & Toupin, S., 2019. What does the notion of "sovereignty" mean when referring to the digital?. *New Media and Society,* 21(10), pp. 2305-2322.

Economy, E. C., 2018. The great firewall of China: Xi Jinping's internet shutdown. *The Guardian,* 29 February.

Fleming, S., 2021. *What is digital sovereignty and why is Europe so interested in it?.* [Online]
Available at: https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/ [Accessed 29 December 2022].

Hern, A., 2015. 'Great Cannon of China' turns internet users into weapon of cyberwar. *The Guardian,* 13 April.

Internet Society, 2022. *Navigating Digital Sovereignty and its Impact on the Internet,* s.l.: Internet Society.org.

Lumen Learning, n.d. *The Peace of Westphalia and Sovereignty.* [Online] Available at: https://courses.lumenlearning.com/atd-herkimer-westerncivilization/chapter/the-peace-of-westphalia-and-sovereignty/
[Accessed 29 December 2022].

Marczak, B. et al., 2015. *China's Great Cannon,* s.l.: The Citizen Lab.

Ministry of Electronics & Information Technology, 2020. *Data Centre Policy 2020,* s.l.: Ministry of Electronics & Information Technology (e-Governance Division).

Musiani, F., 2022. Infrastructuring digital sovereignty: a research agenda for aninfrastructure-based sociology of digital self-determination practices. *Information, Communication and Society,* 25(6), pp. 785-800.

Philpott, D., 2003. *Sovereignty*, s.l.: s.n.

Soni, A., 2015. How people power took on big business in the fight for net neutrality in India. *The Guardian*, 25 May.

Stanford, n.d. *China's Great Firewall.* [Online] Available at: https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html [Accessed 31 December 2022].

The Economist, 2020. Governments are erecting borders for data. *The Economist*, 20 February.

Wu, T. S., 1997. Cyberspace Sovereignty? - The Internet and the International System. *Harvard Journal of Law and Technology,* 10(3), pp. 647-666.