E-GOVERNANCE AND CYBER SECURITY - PROTECTING DEMOCRACY IN A DIGITALISED WORLD

Mr. Mayank Mishra *

Abstract

The power of the internet is undisputed. Even as democracies like India use it to benefit citizenry through systems, structures and processes of e-governance, authoritarian regimes like The People's Republic of China are equally able to harness its power towards extending their reach and control.[1] *This conceptual dissonance in the (perceived) purpose of the internet and practical divergence in its factual uses by states is further complicated by a simple fact - Internet Infrastructure is spread across the planet and across territorial jurisdictions of Westphalian states – democratic, authoritarian and everything in between. Large swathes of the internet and its infrastructure (like undersea cables in international waters) lie in territory that is not owned or controlled by any single state.*

In such an environment, it is imperative that democratic states with open societies like India develop domestic policies and international partnerships to work towards an internet that does not function like some national intranet disseminating official and approved material alone; but instead like the free, democratic and interconnected global network that aids mankind today (or thus far) as part of global commons. Protection and maintenance of 'the internet' – infrastructure as well as cyberspace – should be a policy priority for democracies which may not own it per se but nevertheless hold it on trust (and must continue to do so) for future generations. While purely realistic analysis that invoked interests and realpolitik alone would also find that such an approach and outcome would favour a country like India, it would exist in addition and as supplement to the existing legal bases in international law – like the principles of intergenerational equity and common heritage - that also legitimise policy of free and democratic internet and cyberspace.

* Student: LL.M. @ Amity Law School, Gurugram

[1] Michaelsen and Glasius, Authoritarian Practices in the Digital Age, International Journal of Communication 12 (2018), 3788–3794. Available at: https://ijoc.org/index.php/ijoc/article/viewFile/8536/2458 (Accessed: 15th Nov. 2021.)

LITERATURE REVIEW

Paper Citation: Soham Agarwal & Vice Admiral Pradeep Chauhan, Underwater Communication Cables: Vulnerabilities and Protective Measures Relevant to India (Parts I-II) (Apr. 7, 2021).[2]

Agarwal and Chauhan (2021) provide an excellent (albeit India-centric) overview of the criticality and vulnerabilities of 'Critical Internet Infrastructure (***CII***)'.[3] Part I of their study examines the importance and vulnerability of the physical backbone of 'the internet'. Part II outlines the existing inadequacy of not just domestic Indian law but also international law in protecting identified vulnerabilities in what is a global, distributed and cross-jurisdictional network.

Paper Citation: Marcus Michaelsen and Marlies Glasius, Authoritarian Practices in the Digital Age, International Journal of Communication 12 (2018), 3788–3794.[4]

Michaelsen and Glasius (2018) examine the interplay between authoritarian practices (or practices by authoritarian states) and digital technologies. These practices include but are not limited to censorship, surveillance, interference in sovereign elections using information campaigns etc. Their examination is extended to multilateral, transnational, and public–private settings and contexts. For the purposes of the present paper, Michaelsen and Glasius (2018) convincingly demonstrate the 'dual-use' nature of digital technologies particularly when wielded by authoritarian (or less democratic) nation states. In so doing, they provide basis and rationale to the argument made in the present paper – that democratic states (including India) must take proactive and co-operative steps to ensure protection and maintenance of free and open digital technologies that do not function as mere mouthpieces for centre(s) of power.

Paper Citation: Shanthi Kalathil and Taylor C Boas, The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution, First Monday, Volume 6, Number 8, (6 Aug. 2001).[5]

[2] Agarwal and Chauhan, 2021, Available at: https://maritimeindia.org/underwater-communication-cables-vulnerabilities-and-protective-measures-relevant-to-india-part-1/, https://maritimeindia.org/underwater-communication-cables-vulnerabilities-and-protective-measures-relevant-to-india-part-2/ (Accessed: 16th Nov. 2021).

[3] Section 70 of The Information Technology Act, 2000; Gazette Notification No. G.S.R. 19(E) dated 16th Jan.2014. Available at: https://www.meity.gov.in/writereaddata/files/GSR_19%28E%29_0.pdf (Accessed: 16th Nov. 2021.)

[4] *supra* note 1.

[5] Kalathil and Boas, The Internet and State Control in Authoritarian Regimes: China, Cuba and the Counterrevolution, First Monday, Volume 6, Number 8, 6 Aug. 2001. Available at: https://firstmonday.org/ojs/index.php/fm/article/download/876/785 (Accessed: 15th Nov. 2021.)

Kalathil and Boas (2001) use Cuba and People's Republic of China as examples to highlight how authoritarian and/or illegitimate control can be perpetuated using the internet and its infrastructure. They join extensive existing literature that demonstrates the 'dual-use' nature of the internet and cyberspace as things that can promote as well as suppress civil rights. Kalathil and Boas conclude as follows;

> *Although conventional wisdom often suggests that the Internet is an inherently democratizing technology, many authoritarian regimes have translated a long and successful history of control over previous ICTs into effective control of the Internet. Through reactive strategies that range from the restriction of access to the promotion of self–censorship, authoritarian regimes can successfully restrain the potential challenges posed by various types of Internet use. In addition, these governments can proactively guide the development of the Internet so that the medium extends and consolidates state power.*

They present a strong case because democracies have stakes in *developing* future internet that is free, open, democratic, rules-based, and respectful of (as opposed to weaponised or deployed against) civil rights and liberties.

Paper Citation: Michael Chertoff, The Strategic Significance of the Internet Commons, Strategic Studies Quarterly (Summer 2014).[6]

Chertoff makes a compelling case for viewing the internet and cyberspace – like the High Seas, Outer Space, and Antarctica - as global commons, with attendant and accompanying duties and responsibilities upon national, regional and international actor(s). He advocates for its *"global governance that preserves its freedom and openness while strengthening its security to protect the shared economic and utility value of all nations."*

This view – of the internet as global commons - has been increasingly endorsed and adopted as policy and/or posture by the international community, including democracies like India, and is assumed by the present paper. For instance, the Indian approach to internet governance has been articulated in inter alia the following terms – *"Internet is a shared resource and a global common*

[6] Michael Chertoff, The Strategic Significance of the Internet Commons, Strategic Studies Quarterly (Summer 2014). Available at: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-08_Issue-2/Chertoff.pdf (Accessed on: 15th Nov. 2021.)

available to public. An open, stable and secure Internet, and unhindered access to information and knowledge, is crucial to global connectivity, innovation and economic development."[7]

Paper Citation: Mark Raymond, Puncturing the Myth of the Internet as a Commons, Georgetown Journal of International Affairs, 2013-14, International Engagement on Cyber III: State Building on a New Frontier (2013-14), pp. 53-64.[8]

Raymond (2014) presents a coherent, valid and alternative framework to viewing the internet as a commons (which he argues constitutes thinking that is *"military"* and *"journalistic"*). He agrees that the internet needs to be protected from 'harm'; but by way of proposing a solution to internet governance he argues instead for a *"global commitment on the part of all stakeholders to 'do no harm' to the broader operation of the Internet."* Instead of a conceptual and normative approach that *"'globalizes' internet governance decisions as a matter of principle"*, he advocates for co-operation between the various *"clubs"* of internet governance, whether democratic or otherwise, so as to avoid *"negative externalities resulting from the simultaneous rule-making efforts made by a large number of overlapping and interdependent clubs."*

In theory, consensus and cooperation between competing powers *is* preferable to protracted and costly campaigns of attrition that may or may not succeed. This paper proceeds however to build upon declared positions of the United Nations and multiple democratic states which prefer to conceptualise the internet and cyberspace as global or *digital commons.*[9]

That said, a club-based approach may yet remain relevant to Indian policymakers and their issue-based partnerships under a 'strategic autonomy' framework.

Objective

There are nearly 200 sovereign nation states in the world today, not all of which are democratic. The internet and its infrastructure spans the globe and jurisdictions of multiple nation states. For multiple reasons and to varying degrees, Rule-making and Rule-taking arrangements that

[7] Ministry of External Affairs (GoI), Government of India's Initial Submission to Global Multi-Stakeholder Meeting on the Future of Internet Governance; Sao Paulo, Brazil on April 23-24, 2014. Available at: http://mea.gov.in/Images/pdf/official_submission_to_the_conference.pdf (Accessed: 15th Nov. 2021.)

[8] Mark Raymonds, Puncturing the Myth of the Internet as a Commons, Georgetown Journal of International Affairs, 2013-14, International Engagement on Cyber III: State Building on a New Frontier (2013-14), pp. 53-64. Available at: https://www.jstor.org/stable/43134322 (Accessed: 15th Nov. 2021.)

[9] Nations large and small: a new global deal to deliver global public goods and address major risks, Our Common Agenda (Report of the Secretary General), Chapter IV pp 48, 62-64. Available at: https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf (Accessed: 15th Nov. 2021); Supra n7.

emerged after World War II and the end of the Cold War are undergoing change and flux.[10] In a world that has seriously debated property rights in space settlements for over a decade, 'Ownership' and 'Regulation' of the internet and its infrastructure is expected to emerge as an area where global powers (democratic and others) will engage in legal and military tussle(s) with each other for attrition and dominance.[11]

In this world, it would be prudent for democratic nation states to view the internet – like the environment - as a collective asset (or global common(s)) that they hold on *trust* for countless future generations of citizens. In any democracy under the Rule of Law, public policy as well as law will demand that such an asset and its associated infrastructure be protected inter alia from the purely self-serving machinations of any undemocratic actor, including less democratic (or autocratic, depending on perspective) states like the People's Republic of China.

The objective of this paper is to examine existing and evolving rationales and modalities for the provision of such protection(s) by democratic states – at home and abroad - to the digital world in which their beneficial initiatives of e-governance etc. exist and function. In so doing, it hopes to contribute to existing literature on the need for and measures through which democracy and democratic values may be protected in a digitalised world that continues to digitalise further as well as exponentially.

Part I examines stakes of democratic nation states (like India) in a free and open internet within which people-driven services and initiatives through e-governance etc. function transparently and without undue/unlawful interference.

Part II shows the global reach and expanse of the internet and its physical/hardware as well as logical/software layers. In so doing, one seeks to establish an empirical and logical link between the 'democratic' internet and cyberspace that any 'owner' or other interested party may seek to protect with the cross-border, cross-jurisdictional and transnational threat(s) facing the protectee.

[10] Gregory Chin and Ramesh Thakur, 'Will China change the Rules of Global Order?', The Washington Quarterly 2010 (33:4) pp. 119-138. Available at: https://ciaotest.cc.columbia.edu/journals/twq/v33i4/f_0020820_17304.pdf (Accessed: 16th Nov. 2021); Lavenex et al., Power transitions and the rise of the regulatory state: Global market governance in flux, Regulation & Governance (2021), ISSN 1748-5991. Available at: https://www.econstor.eu/bitstream/10419/242006/1/REGO_REGO12400.pdf) Accessed on: 16th Nov. 2021; Johan Verbeke, A World in Flux, Egmont Institute (2017). Available at: https://www.jstor.org/stable/resrep17412 Accessed on: 16th Nov. 2021.

[11] Wasser and Jobes, Space Settlements, Property Rights, and International Law: Could a Lunar Settlement claim the Lunar Real Estate it needs to survive, 73 J. Air L. & Com. 37 (2008). Available at: https://core.ac.uk/download/pdf/147637461.pdf (Accessed: 16th Nov. 2021.)

Part III outlines some conceptual and/or legal bases that can be legitimately invoked for protection - including through measures that may be extra-territorial as well as coercive - of a free, open and democratic internet.

Part I: Democratic stakes in 'The Internet'.

The power of the internet and its accompanying technologies to benefit citizens and others through good governance and delivery of services is self-evident. There is growing global recognition and acknowledgment of its critical role in not merely the present-day governance of nation states (democratic or otherwise) through the delivery therein of "people-driven services", but also in the future role(s) it is expected to play in an evolving global agenda on Sustainable Development that continues to be defined and developed, including under the 2030 Agenda for Sustainable Development and Sustainable Development Goals.[12] Indeed, the 2030 Agenda commits to a world;

> *[I]n which democracy, good governance and the rule of law, as well as an enabling environment at the national and international levels, are essential for sustainable development, including sustained and inclusive economic growth, social development, environmental protection and the eradication of poverty and hunger.*[13]

The United Nations also found last year that;

> *The top performers in e-government development…. include Denmark, the Republic of Korea, Estonia, Finland, Australia, Sweden, the United Kingdom of Great Britain and Northern Ireland, New Zealand, the United States of America, the Netherlands, Singapore, Iceland, Norway and Japan.*[14]

All these countries are democracies, and effective e-governance is today irretrievably and intrinsically linked to the functioning of a credible modern nation state. India may not thus far

[12] Department of Economic and Social Affairs (United Nations), New global survey shows E-government emerging as a powerful tool, Available at: https://www.un.org/ru/desa/new-global-survey-shows-e-government-emerging-powerful-tool (Accessed: 16th Nov. 2021); Andreea Stoiciu, The Role of e-Governance in Bridging the Digital Divide, Available at: https://www.un.org/en/chronicle/article/role-e-governance-bridging-digital-divide (Accessed on: 16th Nov. 2021.)

[13] Transforming our world: the 2030 Agenda for Sustainable Development, Resolution adopted by The General Assembly on 25th Sept. 2015, page 4 of 35. Available on: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E (Accessed 16th Nov. 2021.)

[14] Department of Economic and Social Affairs (United Nations), E-Government Survey 2020. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (Accessed: 16th Nov. 2021.)

have emerged as a top performer on the UN list, but it is (certainly for the purposes of the present paper) a democratic nation state that continues to work on e-governance initiatives for the benefit of its citizens as well as residents.

While it is clear that democracies have a stake, now and in the future, in a free and open internet and cyberspace, autocratic regimes (like Cuba and The People's Republic of China) also perpetuate authoritarian and/or illegitimate control using the internet and its infrastructure.[15] Indeed, the effectiveness of the internet as a tool of repression suggests that autocratic regimes are *more* and not less likely to introduce 'the internet' to their people(s).[16] As such, this fact too presents a strong *a priori* case for why democracies have a stake in a future internet that continues to be free and open.

Part II: 'The Internet' – Whose and Where?

"Potentially, Internet is everywhere, yet is a single entity; it is both the concept and the thing. Herein lies its strength: the fact it is a single common space, but on a worldwide scale." (Boris Beaude)[17]

Some graphics reproduced below show the global, cross-jurisdictional and distributed nature of the internet and its associated/underlying CII.

Figure 1 has been reproduced from Agarwal and Chauhan (2021), and shows the global map of underwater fibre-optic communication cables or "submarine cables" which form the backbone of today's internet as we know it.[18] While it is true that most of our end connections to the internet are wireless, satellites only account for about 1 percent of human interactions with the internet for many reasons including latency, cost, and the sheer height of telecommunications satellites.[19]

[15] Supra n5; Espen Geelmuyden Rød, Empowering activists or autocrats? The Internet in authoritarian regimes, Journal of Peace Research (2015), Vol. 52 (3), 338–351.

[16] *Ibid.*

[17] Boris Beaude's 'Critical Atlas of Internet' is an excellent tool for the spatial and temporal analysis of the internet and cyberspace, including the social, political, and economic issues therein. It can be accessed at: https://louisedrulhe.fr/internet-atlas/

[18] SEE ALSO N. Starosielski, The Undersea Network, (Durham: Duke University Press, 2015), pp 3-7, 17. Available at: https://blogs.commons.georgetown.edu/engl-711-fall2017/files/2017/08/The-Undersea-Network_Starosielski.pdf (Accessed on: 15th Nov. 2021.

[19] Carol Barford, Key Internet Connections and Locations are at Risk from Rising Seas, American Scientist (2018-11-01), Vol.106 (6), p.3.

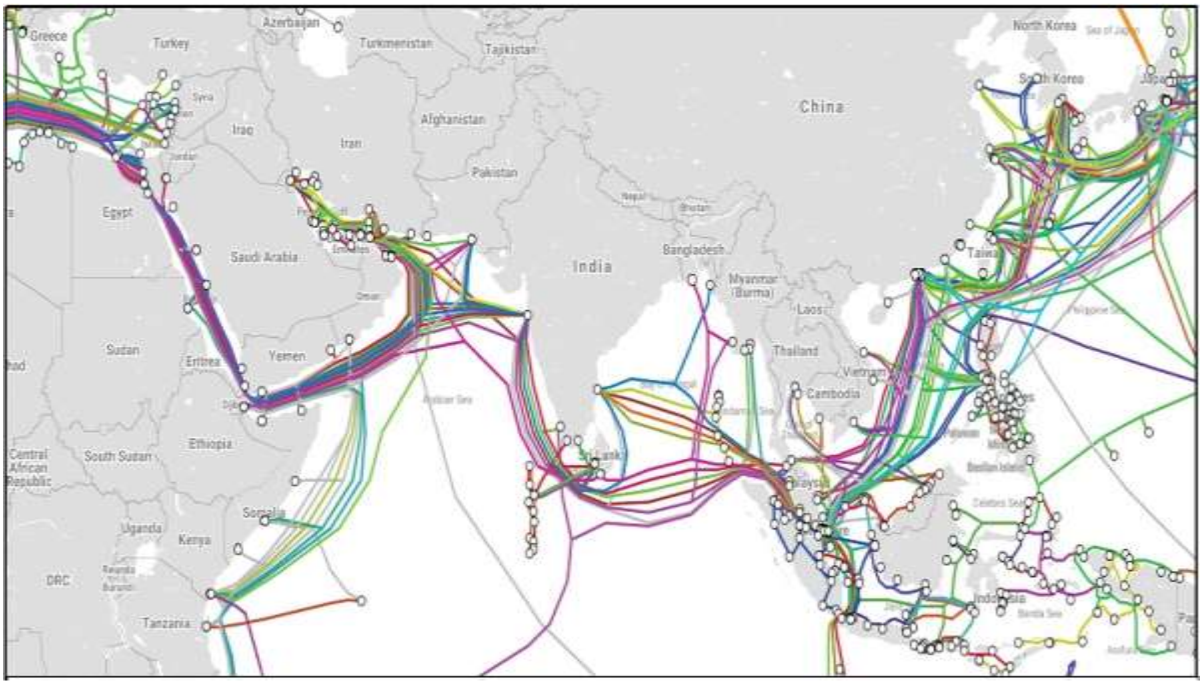

Figure 1

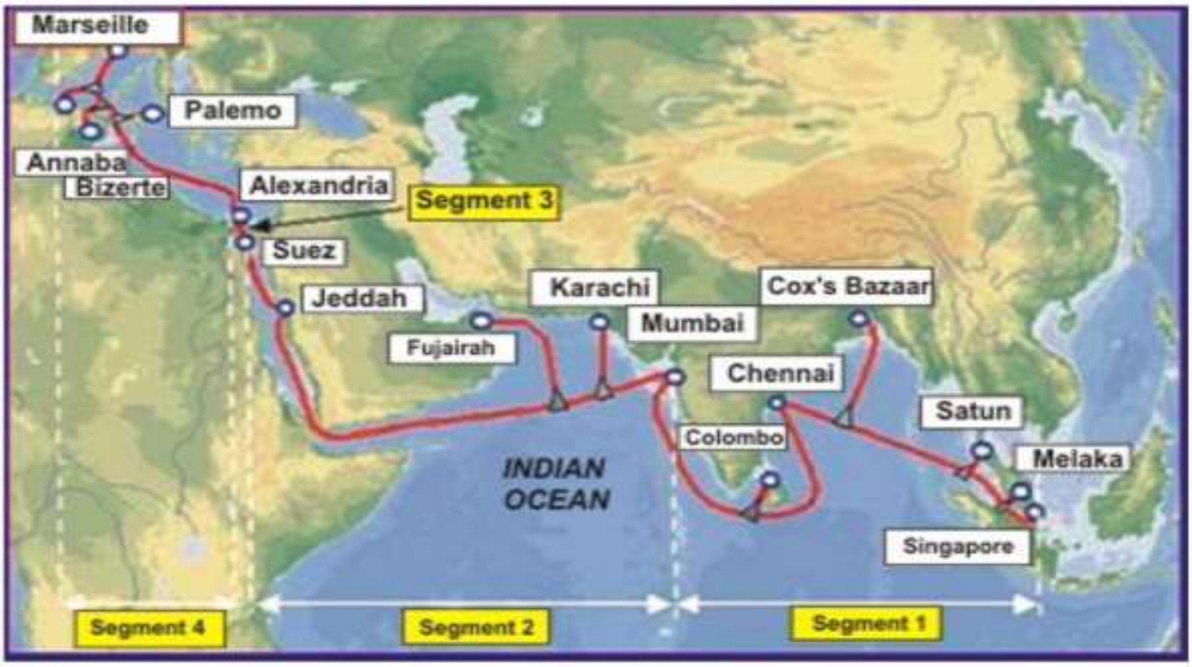

Figure 2

Figure 2 shows the relevant undersea cable network for Asian countries, and linkages with Karachi and West Asia are note-worthy for Asian democracies like India.[20]

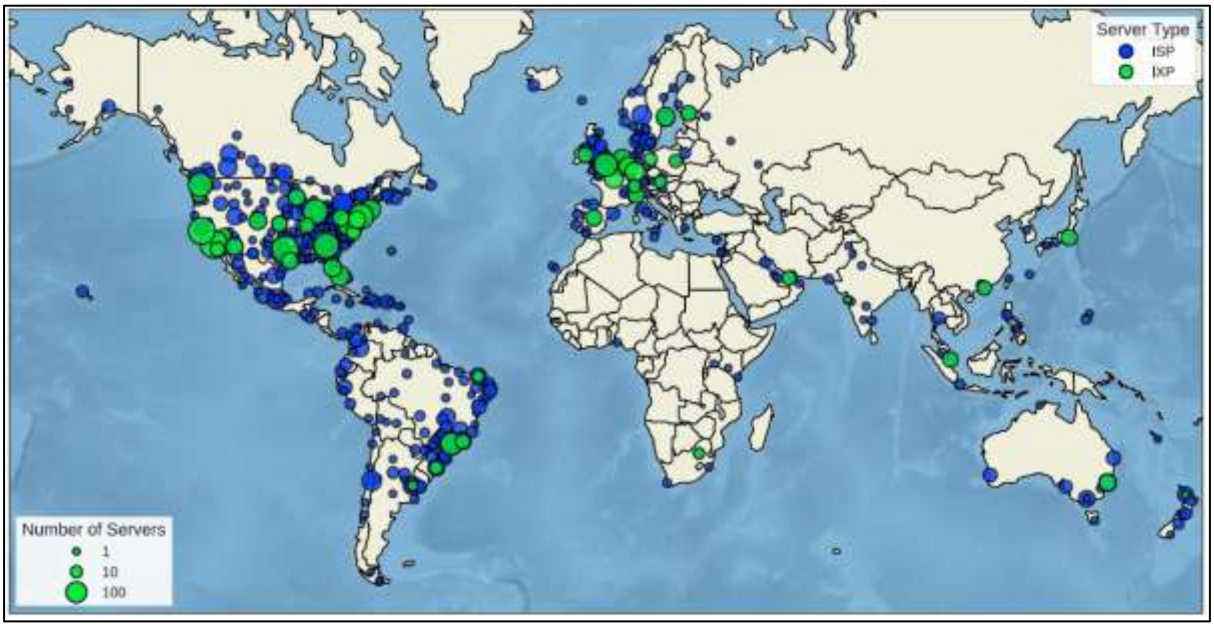

Figure 3

Figure 3 shows the scale and expanse of the Content Delivery Network (CDN) of Netflix which forms the substrate of its physical infrastructure across the world.[21]

More recently, global response to the Covid pandemic through apps and actors has been mapped by researchers and confirms the diffused, distributed, cross-border and multi-agency use(s) – including beneficial and transformative uses - of the internet;

[20] Ali et al., Risk assessment of China-Pakistan Fiber Optic Project (CPFOP) in the light of Multi-Criteria Decision Making (MCDM), Advanced Engineering Informatics 40 (2019), 36-45.

[21] Timm Böttger et al., Open Connect Everywhere: A Glimpse at the Internet Ecosystem through the Lens of the Netflix CDN, ACM SIGCOMM Computer Communication Review, Volume 48 Issue 1 (January 2018), pp 28–34. This author does not endorse depiction therein of Indian borders.

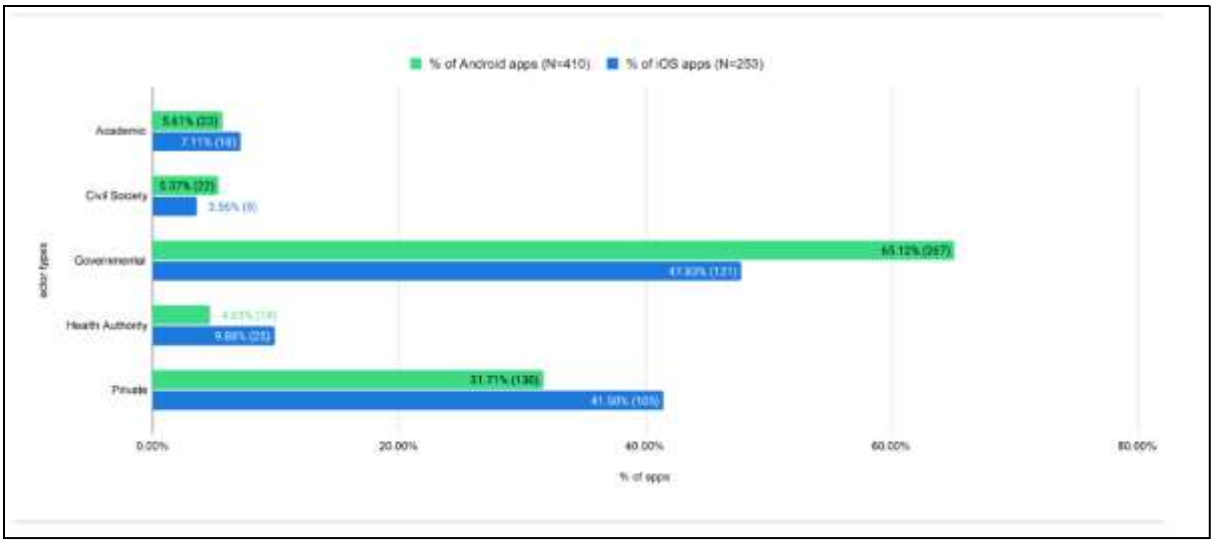

Figure 4

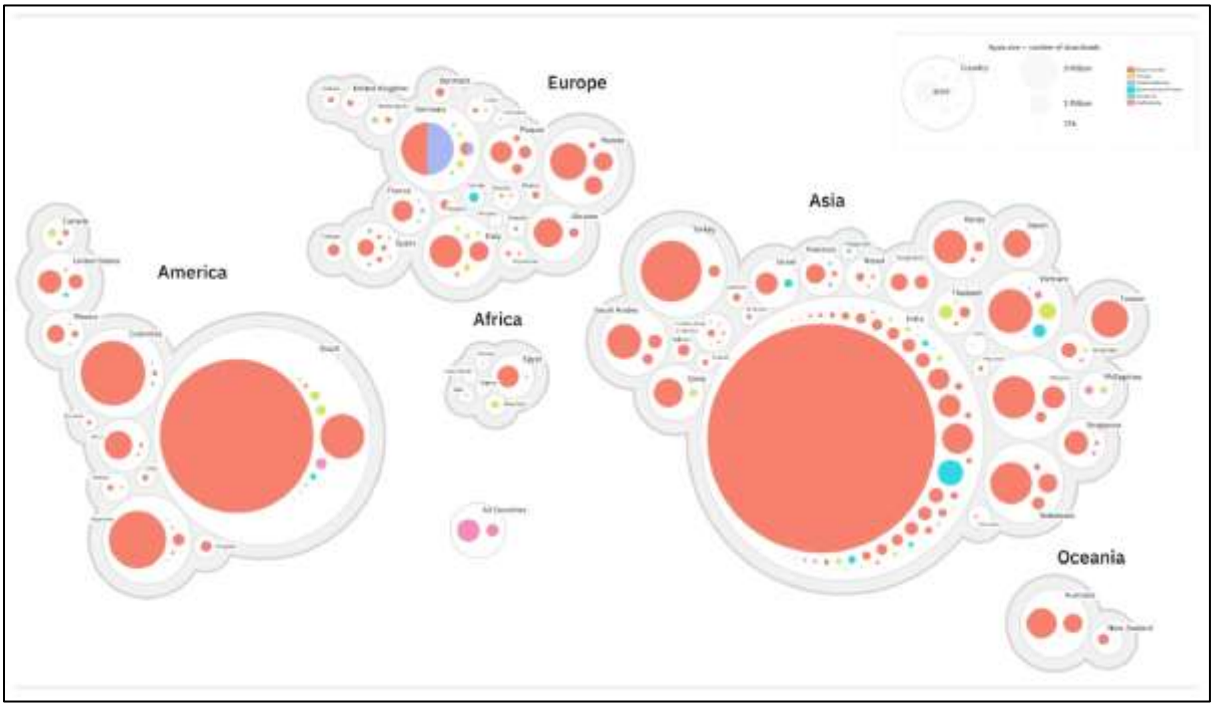

Figure 5

Figure 4 identifies Actor types behind Covid-related apps (Android and iOS), and notes how apps can belong to multiple categories. ***Figure 5*** depicts geographical distribution of Covid-related Android apps by country or region.[22]

Dieter at al found that numerous and unique *"techniques of control determining which apps make it into app stores, how they are positioned and accessed in the stores, who they are developed by, and what kinds of functionality they may have (including restrictions on ads and other economic features)."*[23] Dieter et al also indicate that the distributed nature of the internet and its associated 'platforms' (like app stores, marketplaces etc.) provide *"generative means for a diversity of responses to emerge, with individual apps negotiating these governing conditions as part of their development."*[24]

In addition to cross-border distribution of physical infrastructure, there exists today, mainly for historical reasons, distribution of the internet's soft or logical (i.e. non-physical) infrastructure like DNS servers *across* multiple legal jurisdictions like USA and Europe and also across multiple agencies - from the private not-for-profit public benefit corporation like Internet Corporation for Assigned Names and Numbers or ICANN, to the United States Government's Department of Defense.[25]

One result of this cross-border/cross-jurisdictional nature or sweep of the internet is that the international community and in particular all states – democratic as well as otherwise – find that there is real and substantial *interdependence* behind effective working of their core sectors and by implication and consequence the effective working of their respective governments/states.[26] (Figure 6);

[22] Dieter at al., Pandemic platform governance: Mapping the global ecosystem of COVID-19 response apps, Internet policy review, 2021, Vol.10 (3), p.1-27.

[23] *Ibid* pg. 22.

[24] *Id.*

[25] RSSAC023: History of the Root Server System, Report by ICANN Root Server System Advisory Committee (RSSAC) (4th November 2016), Available at: https://www.icann.org/en/system/files/files/rssac-023-04nov16-en.pdf (Accessed: 15th Nov. 2021.)

[26] Munish Sharma, Securing Critical Information Infrastructure: Global Perspectives and Practices, IDSA Monograph Series No. 60 (April 2017), pp 40-47. Available at: https://idsa.in/system/files/monograph/monograph60.pdf (Accessed: 15th Nov. 2021.)

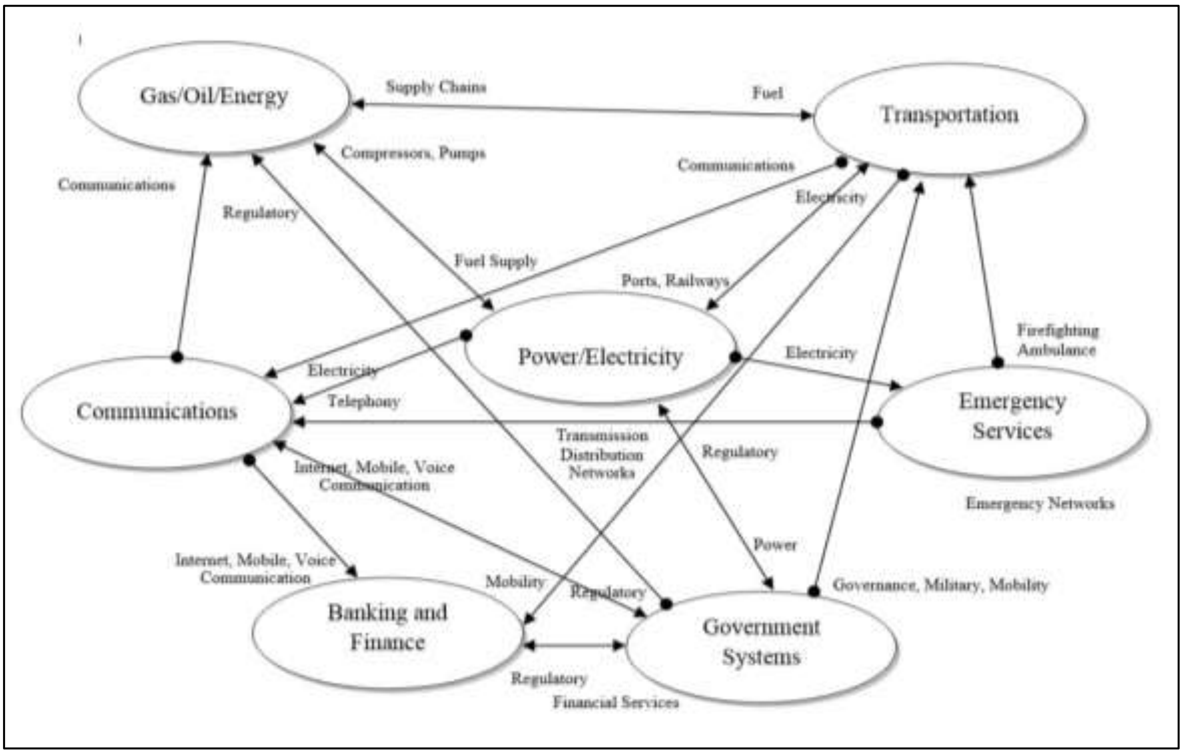

Figure 6

Another result is that the *threats* – real and potential – are also transnational, distributed, and difficult to pre-empt.

These threats can be induced or accidental. Threats induced by humans may be through an insider, an outsider or in collusion. Threats escalate into attacks in multiple ways that continue to evolve – from defacement of websites and identity theft to misinformation campaigns that interfere with sovereign electoral processes.[27]

Furthermore, the internet's distributed and cross-jurisdictional setup offers multiple opportunities to autocratic and/or non-state actors to coerce democratic states into undemocratic arrangements through policies that are a mix of isolation and bargaining with/for *access*. Cyber capabilities can and are used as effective and (relatively) low-cost tools of statecraft, even as their utility over more traditional logic(s) of warfare remains – for now - somewhat limited.[28]

[27] Robles et al., Common Threats and Vulnerabilities of Critical Infrastructures, International Journal of Control and Automation, Vol. 1, No. 1 (2008), pp. 18–19. Available at: http://article.nadiapub.com/IJCA/vol1_no1/3.pdf (Accessed: 15th Nov. 2021); *supra* note 26, pp 51-63.

[28] Quentin E. Hodgson, Understanding and Countering Cyber Coercion, 10th International Conference on Cyber Conflict (2018). Available at: https://www.ccdcoe.org/uploads/2018/10/Art-04-Understanding-and-Countering-

CII requires protection not just from human actors but also natural actors and disasters, including the effects of climate change. To this end, it has been suggested as follows;

> *Future deployments of internet infrastructure will need to consider the impact of climate change. These plans must include consideration of such issues as acquiring and paying for new rights-of-way for laying cables, and costs and projections relating to how populations will move. Other aspects of risk-aware deployment include developing new methods for hardening fibre cables, conduits, and other infrastructure to be more resistant to the severe weather that will be a consequence of climate change.*[29]

The discussion above indicates that on the issue of protecting democracy in a digitalised world, no democracy (including India) is in its own boat. Notwithstanding their respective 'sovereignty'/'strategic autonomy'/'exceptional nature', all democracies are in the same boat.

Part III: Legal Bases for Cross-Jurisdictional Protection

"Our Earth has become a global commons. Cumulatively, actions taken across the world affect its resilience and integrity." (Edith Brown Weiss, 2014)

In light of all that the world has recently seen and learnt from the Covid pandemic (including its origins and management through vaccine(s)), these words ring particularly true.

Like nature, climate and the environment, the internet, cyberspace, and CII as global commons (or digital commons) too deserve and demand comprehensive protection under domestic and international law.

Compartmentalization or fragmentation of the internet and cyberspace into *"loosely coupled islands of connectivity"* is also undesirable because it will deprive today's individuals and future generations

Cyber-Coercion.pdf (Accessed: 15th Nov. 2021); Jon Lindsay and Erik Gartzke, Coercion through Cyberspace: The Stability-Instability Paradox Revisited (25th Aug. 2016), Available at: http://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf (Accessed: 15th Nov. 2021.)

[29] *supra* note 19.

of its full beneficial and transformative potential by *"chip[ping] away to varying degrees at the Internet's enormous capacity to facilitate human progress."*[30]

At present however, there does not exist a *"legal equivalent to the technical interoperability that enables the global internet."*[31] Indeed, it would not be incorrect to say that *"[T]he internet and the online spaces constructed on top of it are human-made – there is no natural law that would prohibit the repartitioning of transnational online spaces along the physical boundaries around which our international governance systems are organised."*[32]

Nevertheless, it is imperative that principles and legal instruments are developed and implemented for protection and sustainability – locally as well as globally - of a free and open internet and cyberspace. Notions and invocations of sovereignty notwithstanding, no nation state *alone* has the power to prevent threats to democratic cyberspace or the capability to ensure its continuing survival.

The principle of inter-generational equity provides *one* good starting point upon which valid analytical jurisprudence on internet governance may be developed.[33]

The principle of inter-generational equity assumes that each generation of human beings receives a legacy *in trust* from the previous generations and holds it in trust for future generations. It lays down duties and obligations of present generations *to* future generations with respect to the use and enjoyment of said legacy that has been inherited by the present generation and is to be passed on to future generations – *as a class and irrespective of nationality* - in no worse condition than

[30] Drake et al., Internet Fragmentation: An Overview, World Economic Forum (Jan 2016), pg 3. Available at: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (Accessed: 15th Nov. 2021.)

[31] Paul Fehlinger, Cyberspace fragmentation: an internet governance debate beyond infrastructure, Internet & Jurisdiction Policy Network (17th Apr 2014) (Paris). Available at: https://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266 (Accessed: 15th Nov. 2021.)

[32] *Ibid.*

[33] Others include 'common concern of humankind', and 'common heritage of mankind'. SEE Bowling et al., The Common Concern of Humankind: A Potential Framework for a New International Legally Binding Instrument on the Conservation and Sustainable Use of Marine Biological Diversity in the High Seas. Available at: https://www.un.org/depts/los/biodiversity/prepcom_files/BowlingPiersonandRatte_Common_Concern.pdf (Accessed: 15th Nov. 2021); Werle et al., The future of ocean governance and capacity development: essays in honor of Elisabeth Mann Borgese (1918–2002), International Ocean Institute (Canada, 2018) , pg 216, 218. Available at: https://library.oapen.org/bitstream/handle/20.500.12657/37811/9789004380271_webready_content_text.pdf?sequence=1&isAllowed=y (Accessed: 15th Nov. 2021); Bellinkx et al., Addressing Climate Change through International Human Rights Law: From (Extra) Territoriality to Common Concern of Humankind, Transnational environmental law, 2021-06-24, p.1-25.

it was received. In so doing, this principle seeks to achieve an equitable balance between the needs of present and future generations.

In the context of a free and open internet, this principle indicates that we (particularly democratic peoples under Rule of Law) are all trustees, custodians and beneficiaries of a free and open internet. We are all partners in caring for and using the digital commons.

Weiss articulated it thus;

> *In the context of future generations, one can argue that future generations have rights and the present generation has obligations to respect those rights. Rights of future generations are not individual rights. Rather they are generational rights, which can be usefully conceived only at a group level. They are in the nature group or collectively held rights in relation to other generations – past, present, and future. They exist regardless of the number and identity of the people who exist in each generation.*[34]

This principle is widely invoked in the debate on climate change and international environmental law, and is an essential element of the broader principle of Sustainable Development.[35] It forms the basis of '***UNESCO Declaration on the Responsibilities of the Present Generations Towards Future Generations***'.[36] Many democratic jurisdictions, including the Indian Supreme Court, have invoked and applied this principle in their jurisdiction(s).[37]

While it is true that application in domestic law does not *ipso facto* imply existence of and/or application as a rule of international law, increasing application of the principle by countries

[34] Edith Weiss, Nature and the Law: The Global Commons and the Common Concern of Humankind, Pontifical Academy of Sciences, Extra Series 41, Vatican City (2014), pg 5. Available at: http://www.pas.va/content/dam/accademia/pdf/es41/es41-brownweiss.pdf (Accessed: 15th Nov. 2021.)

[35] Edith Weiss, In Fairness to Future Generations and Sustainable Development, Environment: Science and Policy for Sustainable Development, 1990-04-01, Vol.32 (3), p.6-31; Article 3(1) of United Nations Framework Convention on Climate Change (UNFCCC); Sohn and Weiss, Intergenerational Equity in International Law, Proceedings of the Annual Meeting (American Society of International Law), April 8-11, 1987, Vol. 81 (April 8-11, 1987), pp. 126-133.

[36] Adopted on 12th Nov. 1997 by the General Conference of UNESCO at its 29th session. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000110827 (Accessed: 15th Nov. 2021.)

[37] *State of Himachal Pradesh v Ganesh Wood Products,* AIR 1996 SC 149, 1995 SCC (6) 363; *K .Guruprasad Rao v State of Karnataka*, (2013) 8 SCC 418; *Court on Its Own Motion v. Union of India ,* SuoMotu Writ Petition (civil) No. 284 of 2012, (2013) 1 MLJ 639 (SC); *Kinkri Devi And Anr. v State Of Himachal Pradesh And Ors. AIR 1988 HP 4*; *Vellore Citizens Welfare Forum v. Union of India* (Tamil Nadu Tanneries Case) (1996) 5 SCC 647; Article 6 of the New South Wales' Protection of the Environment Administration Act 1991; *infra* note 38.

(especially democracies) does provide evidence that the principle is *"becoming entrenched as [a] customary norm of international law"*.[38]

It must also be pointed out that no general international law instrument thus far defines the core elements of this principle, nor has it (thus far) formed the legal basis for resolution of a dispute before a Court.[39] Even so, this principle can be considered a 'guiding principle' in the application of substantive norms - including existing treaty obligations - under international law.[40]

Conclusion

Indian policymakers should note that the protective principle can and ought to be extended to CII. Domestic Indian law must extend and/or exercise (as required) its prescriptive jurisdiction over CII defined through due process. CII under Indian law must include critical non-military internet cables in international waters and physical servers located in extra-territorial/foreign locations.

Democratic states should note that any possibility or prospect of a general treaty on internet governance is remote. Instead of tackling broad principles of sovereignty etc. as a first step, democracies may find benefit(s) in first formulating and implementing agreements on limited rules - like due diligence norms, and a prohibition (universal, mutual/bilateral or multilateral) on attacking CII.[41]

Democratic states must band together for the protection of a free and open internet against determined and resourceful autocracies that seek to regulate and/or undermine *as a matter of state policy* the internet's inherent power(s) - including its power to set people(s) free. To this end, there should be development and operationalization of combined policy and regulatory responses (and periodic reviews thereof) by democratic states.

[38] DeMarco et al., Case Note: Supreme Court of Canada (30 October 2003), Imperial Oil ltd v. Quebec (Minister of the Environment), RECIEL 13 (1) 2004, pg 112.

[39] Catherine Redgwell, Principles and Emerging Norms in International Law: Intra- and Inter-generational Equity (24th March 2016), in The Oxford Handbook of International Climate Change Law (Part III Ch.9).

[40] *Ibid.*

[41] Harriet Moynihan, The Application of International Law to State Cyber attacks, Chatham House (2nd Dec. 2019), pg 58. Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf (Accessed: 15th Nov. 2021.)

The principles and modalities for such 'digital cooperation' have been summarised through outreach and discussions with stakeholders by the United Nations, and deserve the attention of policymakers in democratic states like India.[42]

Meaningful digital cooperation among democracies continues to be impeded for instance by ambiguity in definition(s) of an 'international CII', such as it is. Does the word 'international' indicate ownership of and/or by the international community as a whole; or does it refer merely to the cross-jurisdictional/cross-border nature of *some* critical CII? Adamson opined that the absence of any physical CII (separate from logical or soft CII like TCP/IP and DNS protocols that equally constitute 'backbone' of the internet) that *does* belong to the international community as a whole gives credence to the latter interpretation.[43] Adamson's analysis dates back to 2017, but this question remains worthy of further examination today.

Other questions that deserve examination are whether cyber operations - and in particular state-sponsored cyber operations - constitute an internationally wrongful act or behaviour under international law; and the threshold at which any 'intervention' would be justified in law.[44]

[42] The Age of Digital Interdependence, Report of the UN Secretary-General's High-level Panel on Digital Cooperation, Annexure VI pg 39. Available at: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (Accessed: 15th Nov. 2021.)

[43] Liisi Adamson, International Critical ICT Infrastructure and Norms? Available at: https://ict4peace.org/wp-content/uploads/2017/02/Adamson-CI-and-data-integrity.pdf (Accessed on: 15th Nov. 2021.)

[44] *supra* note 44.