Page 1473 - 1477 **DOI:** *https://doij.org/10.10000/IJLMH.114537*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 2

2023

© 2023 International Journal of Law Management & Humanities

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for "free" and "open access" by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **Gyan@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Cyberspace as a Non-Territorial Virtual Space: Unraveling the Conundrum of State Sovereignty in the Cyberspace as a New-Domain

PARTH DEWAN[1]

ABSTRACT

Cyberspace has grown and altered many facets of human life during the course of last three-decades. Governments, organisations, and general public have all greatly utilised the potential that cyberspace offers. The established political, social, and economic systems of the international order have been put to test by the internet. Parallel to these unprecedented changes, the rise of cyberspace has posed significant risks to both individual(s) and societal security. Key national infrastructure is vulnerable to cyberattacks, cybercrime and cyber-espionage endangers the world economy; whereas hackers intimidate people. Armed forces, terrorist organisations, and even "lone-individuals" now have all the potential to wage cyberattacks against vital infrastructure as well as military networks. All of this, raises the critical question of whether or not, is it possible for individual states to regulate cyberspace as a non-territorial virtual space?

This Reflection Article, builds upon this critical question and, undertakes a "global-commons" approach for tackling the contemporary security challenges in the cyberspace!

Keywords: *State Sovereignty, Cyberspace, Global Commons, International Regulation of Cyberspace.*

I. INTRODUCTION

Cyberspace has grown and altered many facets of human life during the course of last three-decades. Governments, organisations, and general public have all greatly utilised the potential that cyberspace offers. The established political, social, and economic systems of the international order have been put to test by the internet. Parallel to these unprecedented changes, the rise of cyberspace has posed significant risks to both individual(s) and societal security. [2] Key national infrastructure is vulnerable to cyberattacks, cybercrime and cyber-

[1] Author is an exchange student at the Universidad Pontificia Comillas, Madrid (Spain). Currently studying at O.P. Jindal Global University, India.

[2] "Betz, AJ & Marks, S 2015, 'Cyberspace and the state: toward a strategy for security in cyberspace' International Institute for Strategic Analysis, Oxon"

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

espionage endangers the world economy; whereas hackers intimidate people. Armed forces, terrorist organisations, and even "lone-individuals" now have all the potential to wage cyberattacks against vital infrastructure as well as military networks. [3] **All of this, raises the critical question of whether or not, is it possible for individual states to regulate cyberspace as a non-territorial virtual space as it is?**

This Reflection Article focuses onto the research paper by **Mr. A. Liaropoulos** (titled **"Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction")** attempting to critique-counter its central argumentation, which establishes cyberspace in common with other territorial domains like (land, sea, air and outer space). In this paper, I undertake a "global-commons approach" towards the cyberspace, shedding light upon cyberspace's inherent issue of misalignment i.e., "…the mismatch between transnational space for global interaction created by the internet and the territorial jurisdictions of national governments…" [4]. As, the internet conjoins the world of governance into a single entity; sovereignty breaks it into 196 pieces! Towards the end of this paper, we shall also evaluate the efficacy of this approach in a 'sand-box' discussion in **tackling threats posed by cyberspace for adding credibility & reliability to our approach!**

II. SOVEREIGNTY IN CYBERSPACE: THE 'WHYS' & THE 'HOWS' BY MR. A LIAROPOULOS

Lately, there has been a growing trend that the issues and complexities viz-a-viz the Internet governance support a move towards sovereignty in cyberspace. **Mr. A Liaropoulos**, certainly upholding a similar viewpoint, sets the stage in his paper for state sovereignty in cyberspace. The paper vividly reflects upon some of the recent cyber-conflicts such as: the Denial-of-Service (DOS) attacks on Estonia (triggered by Russia) crippling its IT infrastructure. [5]

Parallel to which, the author puts forth the idea that, "…anyone attempting to untangle the complexities of cyberspace cannot afford to ignore the concept of sovereignty…". Highlighting that, in accordance with the United Nation's principle of sovereign equality it is the top priority of all the international organizations and states to protect state sovereignty. And, for preserving one's **Domestic Sovereignty** it is indispensable for the state to control

[3] "Carr, J 2011, 'Overhauling cyber warfare' O'Reilly Sebastopol"
[4] "Dr. M. Mueller, 'Sovereignty and Cyberspace: Organizations and Cyber Governance' 5th Annual Vincent and Ellinor Ostrom Guest Lecture"
[5] "Blank, S 2008, 'Cyber- war 1: is Europe's first information war a new kind of war?' vol. 23, no. 4, pp. 227-57"

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

what passes its territory, otherwise it shall fail in regulating what happens within them. [6] **Mr. A Liaropoulos,** elucidates upon four-ways in which sovereignty can be understood and emphasizes particularly upon the **Interdependence Sovereignty** (involving trans-border activities, movement of people, commodities and ideas) which ought to be systematically regulated for ensuring domestic sovereignty. The paper then hypothesizes, that sovereignty in cyberspace is possible on the grounds that, '…cyberspace is bounded by existing physical structures, making its critical infrastructure sectionally based and therefore not resistant from state sovereignty…'. **Conclusively suggesting, that sovereignty in the cyberspace is a viable & effective solution for contemporary issues viz-a-viz the cybersecurity.[7]**

III. DEBUNKING THE IDEA OF STATE SOVEREIGNTY IN CYBERSPACE

Unequivocally, it is the need of the hour that a regulatory framework is laid down for the systematic regulation of the cyberspace. Having said that, the efficacy of state sovereignty in tackling these challenges can be challenged on both practical intellectual grounds. Because inevitably, **sovereignty in cyberspace could only be attained by giving-up the majority of what makes the Internet valuable. Though not entirely impossible, but definitely undesirable!** Three fundamentally strong arguments have been analyzed here-under for adding credibility to the said proposition:

1) For a very long time, the high seas have been considered to not be subjected to state sovereignty claims. In fact, the US Government and other maritime authorities have argued in favor of right to unrestricted navigation in light what they consider it as, **"excessive claims by other states of jurisdiction over ocean space or international passage"**. Furthermore, as stated in the Outer Space Treaty (passed in 1967) it bans its signatories from installing nuclear weapons in space and, the Article-2 explicitly states that, **"…outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty…". [8]** Sea, air, and space, have been recognized as "global-commons" by the international community as, they bring economic benefits to various nations and is something upon which every nation depends. The point here being that, a "global-commons" approach is neither unprecedented nor unimaginable for certain domains; and cyberspace is one of those virtual domains!

[6] "Krasner, KD 2001, Sovereignty: organized hypocrisy, Princeton University Press, New Jersey"
[7] "Wu, TS 1997, 'Cyberspace sovereignty?, the cyberspace and the international apparatus', Harvard JL & Technology, vol. 11, no. 2, pp. 647-66"
[8] "Scott Jasper, 'Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security' Press 2012 JSTOR"

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

2) The Internet Standardized Protocols which enable the users have access to data and services with easy from across the length & breadth of the globe, are 'open source, non-exclusive and non-proprietary'. These protocols create a "global-commons" as anyone can implement them and pragmatically allow unlimited connection of networks **(the standard allows for around 3.7 billion AS numbers)**. The AS doesn't operate in a physical layer phenomenon and gives rise to a non-territorial virtual space. [9] Though hardware support is requisite for running the software, transmitting and storing data, as soon as these protocols are put-to work, the constitute a part of the non-geographic virtual space. Whatever territories or restrictions that exist in the cyberspace are outlined and regulated by software instructions which can come from anywhere around the world. For becoming a **"highly-restrictive" only national network**, a state shall have to cut off all the connections of its gateways from global stations; without which it shall not be able to connect to the global-space. **And certainly, the state's assets got to be a part of this "global-commons" (i.e., cyberspace) for deriving benefits of globalization, trade, connectivity and et cetera. [10]**

3) Ultimately, security issues in the cyberspace are not restricted territorially or nationally; they embrace the virtual arena in totality. **Data packets may pose cyber-threats** regardless of the fact whether they come from inside or outside the country's territory. In fact, data packets capable of causing security issues, can be generated by agents from outside the territory (with domestic origin) if they have remote over the domestic system. Threats, intrusions and malware can arise from any part of the world. Ibid As, it is the AS territory and the protection of information assets-**not jurisdictional boundaries**- that actually matters! Once one is dealing with **cross-border connectivity and instantaneous-invisible action(s) from across the so-called "network boundaries", there doesn't exist a pertinent distinction the state actors and non-state actors**. As a matter of fact, the State actors and the criminals undertake similar kinds of technique and attacks. Ibid

IV. CONCLUSION: MAKING A CASE FOR "GLOBAL SOVEREIGN"

Now, as we have aptly reflected upon the apparent futility of sovereignty in cyberspace in tackling the contemporary security issues, we have also parallelly made a case for a distinct approach which could serve our purpose. For which specifically, we ought to finally shed light upon the advantages that accrue from deserting the idea of **"sovereignty in cyberspace"**.

[9] "Florian Kriener, 'Cyber-Space, Sovereignty and Nuances of International Law-Formulation' Volkerrechtsblog"
[10] "G. Stang, 'Cyberspace ought to be seen as a Global Commons' South Asia Journal 3rd February 2021"

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]

i. We can all agree upon how terrible it shall be if the U.S. or any powerful state alike claimed sovereignty over the outer space or seas. Such a claim could only be upheld by the use of constant military force. Turning away from sovereignty demands the states to acknowledge their co-existence in this boundless cyberspace-especially with corporations and civil societies. **This is indispensable for mitigating inter-state conflict as, no state can justify their actions of absolute authority over a distinct "piece" of world.**

ii. The idea of "global-commons" in the cyberspace enhances the significance of global connectivity and harmony in reference to other common ambitions. It propounds in favor of the global internet users' interest, for an open and secure global cyberspace; acknowledging the significance of **supporting economic growth, enhancing human rights and development in technology**.

iii. Finally, a non-sovereign approach puts both-state & non-state actors- on the same horizon, who are equal creators and contributors to the cyberspace. Because, the State apparently doesn't uphold a "special status" and is just another participant in the network of networks.

Such an approach, strikes the right balance between rigidity & flexibility where the position of civil society is strengthened and simultaneously, the domestic regulatory apparatus remains un-interfered.

"This Reflection Paper, unequivocally corroborates for the construction of a new international order in light of the contemporary security threats. However, this paper objects to the erroneous interpretation of a crucial distinction by Mr. A Liaropoulos which is that "...there doesn't exist a national cyberspace for supreme regulation. Instead, there exists a shared global cyberspace which ought to be regulated accordingly! **Ibid**

*****

© 2023. International Journal of Law Management & Humanities [ISSN 2581-5369]