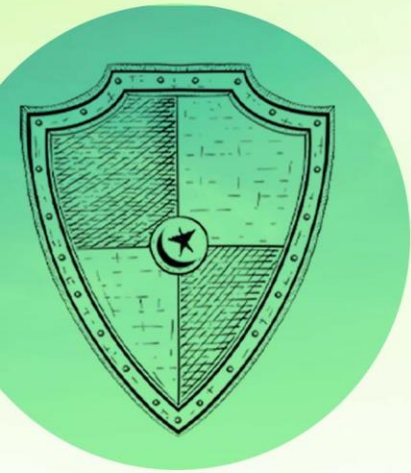




CENTRE for AEROSPACE & SECURITY STUDIES



Governing the Digital Frontier: Cyberspace as the New Global Common

Air Marshal Zahid Mehmood (Retd)

Director

Working Paper



© Centre for Aerospace & Security Studies

June 2024

All rights reserved. No part of this Publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the Editor/Publisher.

Opinions expressed are those of the author/s and do not necessarily reflect the views of the Centre. Complete responsibility for factual accuracy of the data presented and bibliographic citations lie entirely with the author/s. CASS has a strict zero tolerance plagiarism policy.

President

Air Marshal Javaid Ahmed (Retd)

Edited by:

Sarah Siddiq Aneel

Layout

Hira Mumtaz

All correspondence pertaining to this publication should be addressed to CASS, Islamabad, through post or email at the following address:

Centre for Aerospace & Security Studies

☎ +92 051 5405011

✉ cass.thinkers@casstt.com

f [cass.thinkers](https://www.facebook.com/cass.thinkers)

@ [cassthinkers](https://www.instagram.com/cassthinkers)

✕ [@CassThinkers](https://twitter.com/CassThinkers)

in [Centre for Aerospace & Security Studies](https://www.linkedin.com/company/centre-for-aerospace-and-security-studies)



CENTRE for AEROSPACE & SECURITY STUDIES

Governing the Digital Frontier: Cyberspace as the New Global Common

Working Paper

Air Marshal Zahid Mehmood (Retd)

Director

TABLE OF CONTENTS

Abstract	1
Introduction	2
Understanding the Global Commons	3
Cyberspace as a Global Common	5
Cyberspace and Global Governance	8
Analysis	18
Future Outlook	21

Abstract

Cyberspace is commonly defined as 'the online world of computer networks, particularly the Internet.' Its utilisation spans both personal and professional domains, encompassing activities from entertainment and communication to business and the arts, thereby accommodating the full spectrum of contemporary human endeavours. The users of cyberspace include nation-states, corporations, educational institutions, and individuals, among others. The ubiquitous nature of this emergent global common presents unique challenges and a multitude of associated issues. This Working Paper aims to identify the commonalities and differences between cyberspace and other global commons. It will explore the issues related to both direct and indirect threats to national and international security posed by or through cyberspace. Towards the end, the paper will examine the governance of cyberspace and present salient conclusions to mitigate the threats emerging from this domain.

Keywords: Cyberspace, Global Commons, Governance, Cyber Threats.

Introduction

In modern times, the concept of 'Global Commons' has expanded beyond physical domains and natural resources to encompass the digital realm. 'Cyberspace', a virtual environment where information flows freely across borders, has become the newest and a critical global common. This *Working Paper* explores the nature of global commons in the context of cyberspace, discussing its characteristics as an open, accessible, and interconnected domain that serves as a prime example of a shared global resource. The discussion will begin with a general introduction to global commons, highlighting the similarities and differences between physical global commons and cyberspace. Unlike traditional commons, cyberspace lacks physical boundaries, enabling instantaneous communication, economic transactions, and information dissemination on a global scale. This inherent openness and accessibility present both opportunities and challenges, necessitating robust governance frameworks to manage its complexities effectively.

Central to this examination will be an analysis of the current state of global governance of cyberspace. Based on extensive review of existing literature and an analysis of real-world examples, the paper will review international efforts, treaties, and organisations aimed at regulating cyberspace, addressing issues such as privacy, standards, and cyber sovereignty. It will assess the strengths and weaknesses of existing governance structures in balancing the need for innovation and collaboration with the imperative of security and stability. Furthermore, the paper will explore the evolving landscape of cyber threats to national security. It will discuss state-sponsored cyber threats and the exploitation of vulnerabilities in critical infrastructure. By examining case studies, the paper will elucidate the complexities and consequences of these threats, underscoring the urgency of coordinated international responses. Finally, the study will forecast future trends in the global governance of cyberspace.



Understanding the Global Commons

Global Commons

The earliest use of the term 'The Commons' can be traced back to 1968 in an article by Garrett Hardin, titled 'The Tragedy of the Commons.'¹ Hardin employed the example of unregulated grazing grounds used by multiple herders. He argued that for the pasture to remain beneficial for all, grazing must be regulated and the size of herds controlled underscoring the necessity of collective management and regulation to prevent the depletion of shared resources.

Traditionally, a global common is defined as a natural domain or area not governed by or under the jurisdiction of a single nation or political entity. Susan Buck defines these commons as 'natural assets outside national jurisdictions, such as the oceans, atmosphere, outer space, and the Antarctic.'² These resource domains are accessible to all nations under legal frameworks. Antarctica, the high seas, and outer space are generally accepted as global commons. These commons are intended to bring economic benefits to nations, facilitate trade, travel, and business opportunities. In addition to these economic advantages, global commons provide avenues for advancing human knowledge through exploration and experimentation.

Over the past four decades, there has been an ongoing global debate regarding the concept of global commons. A significant portion of the discussion has focused on the nature of global commons and the methods required to regulate and control the variables involved, as indicated by Hardin. Nobel Prize recipient Elinor Ostrom noted that 'human motivation is complex, the rules governing real commons do not always permit free access to everyone, and the resource systems themselves have dynamics that influence their response to human use.'³

An important aspect to consider is that the agreed-upon global commons cannot be governed by any single state or nation. Firstly, most countries lack the capacity to effectively govern and exercise control over these vast and often inaccessible domains on their own. Secondly, opposing and diverse claims over such areas have the potential to escalate into international conflicts. Lastly, it is in the mutual interest of

¹ Garrett Hardin, "The Tragedy of the Commons," *Science* 162, no. 3589 (1968): 1243-1248.

² Susan Buck, *The Global Commons: An Introduction* (New York: Routledge, 1998), 5-6.

³ Thomas Dietz et al., *The Drama of the Commons* (Washington, D.C.: National Academy Press, 2002), 3.

states to cooperate and ensure equitable access to these areas, promoting shared benefits and reducing the risk of disputes.

Outer space and the open seas are quintessential examples of global commons. These domains do not fall under the jurisdiction of any single nation and are open for exploration and exploitation. Specific international treaties have been established to regulate these two domains. The 'United Nations Convention on the Law of the Sea' (UNCLOS), enacted in 1994,⁴ governs the open seas, while the 'Outer Space Treaty' (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies) came into force in 1967.⁵

In general, these treaties or pacts are attempts to regulate the global commons so that all nations can operate under common and binding international regimes. This aims to avoid conflict and contention and ensure that every nation can benefit from the global commons. However, in practice, they have often failed to fulfill their promised objectives. For instance, there is ongoing debate over the adoption of UNCLOS III by the United States (US). As of 2013, UNCLOS III had been implemented by 166 countries and the European Union (EU),⁶ while the US, Colombia, Israel, Peru, and Türkiye have not yet ratified the treaty.

Despite these stumbling blocks, nations continue to collaborate and cooperate by reacting collectively to potential threats to peace, stability, and access to the open seas. For example, in 2009, all nations agreed that Somali piracy posed a significant threat to the passage of trade in the open seas, with an estimated cost to the global economy of USD 18 billion per year.⁷ In response, NATO launched 'Operation Allied Protector' and 'Operation Ocean Shield,' aimed at using armed naval forces to patrol the Somali coast and mitigate the threat.⁸

⁴ United Nations, *United Nations Convention on the Law of the Sea* (New York: United Nations), 10, accessed June 30, 2024, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

⁵ United Nations, *United Nations Treaties and Principles on Outer Space* (New York: United Nations, 2002), 12, <https://www.unoosa.org/pdf/publications/STSPACE11E.pdf>.

⁶ Council on Foreign Relations, *The Global Oceans Regime*, report (New York, June 19, 2023), <https://www.cfr.org/report/global-oceans-regime>.

⁷ Ibid.

⁸ Michael Horowitz, "A Common Future? NATO and the Protection of the Commons," (paper, Transatlantic Paper Series no. 3, The Chicago Council of Global Affairs, 2010), https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Trans-Atlantic_Papers_3-Horowitz.pdf.



A similar case of interference and disruption of trade occurred in the Malacca and Singapore Straits. Annually, 60,000 vessels pass through these straits, with 30 percent of world trade and 50 percent of world energy transiting through these relatively narrow passages.⁹ International and regional collaboration has been crucial to ensuring the safety and preservation of global trade in these vital waterways.

In the case of outer space, the Committee on the Peaceful Uses of Outer Space (COPUOS) was established in 1959. Its aim was to create international agreements on access to outer space. The 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space', signed in 1967, is considered the most widely accepted treaty, with 100 nations as signatories. This treaty essentially mandates that the exploration of outer space should benefit all countries, prohibits the placement of nuclear weapons in space, and ensures that outer space remains free for exploration and use by all nations.¹⁰

From the above, it can be concluded that a generalised definition of the global commons does exist. However, each recognised global common is vastly different in form and function. The promised benefits of these commons can be reaped by all if all parties agree on and adhere to the established rules.

Cyberspace as a Global Common

The widespread and global use of computers in a networked environment began in the early 1960s. The term 'cyberspace' does not have a universally accepted definition, with various scholars and organisations providing their own interpretations.¹¹ According to the U.S. Department of Defense, cyberspace is 'a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.' Conversely, the Russian-American Cyber Security Summit described cyberspace as 'an electronic

⁹ "World Choke Points," *U.S. Energy Information Administration*, accessed June 24, 2024, <http://www.eia.gov/countries/regions-topics.cfm?fips=wotc&trk=p3>.

¹⁰ "Committee on the Peaceful Uses of Outer Space: 2024, Sixty-seventh session (19-28 June 2024)" *United Nations Office for Outer Space Affairs*, accessed June 24, 2024, <https://www.unoosa.org/oosa/en/ourwork/copuos/2024/index.html>.

¹¹ Uche Mbanaso and Emmanuel S. Dandaura, "The Cyberspace: Redefining A New World," *IOSR Journal of Computer Engineering* 17, no. 3 (May-June 2015): 17-24, doi: 10.9790/0661-17361724.

medium through which information is created, transmitted, received, stored, processed, and deleted.¹²

Due to tremendous technological advances in computer hardware and software, the entire global population and every nation are now, in one way or another, dependent on or affected by cyberspace. As of 2023, approximately 5.4 billion people, or 67 percent of the world's population, are using the Internet.¹³

Overview

By the 1990s, researchers such as Charlotte Hess, started writing about the Internet as a common, using the same analogy as Garret Hardin.¹⁴ In 2001, Stanford Law Professor Lawrence Lessig wrote about creation of an 'Internet Commons'.¹⁵ Since then, a number of scholars have studied and written on the subject. While most of the available writings tend to agree that cyberspace has more similarities with the other recognised global commons, some have argued that the differences outweigh the similarities. Most notably, Mark Raymond argues against the notion of the 'Internet' as a global common.¹⁶ Raymond presents a compelling case by asserting that the usual control mechanisms and characteristics shared by other global commons do not apply to the Internet. He cites examples where states exercise strict control over the Internet within their own territories, such as Iran and China.

The Internet is a major element of cyberspace, but the terms are not interchangeable. Cyberspace encompasses a broader scope, including various digital communication environments beyond the Internet accessible to the common person. In other words, 'cyberspace' can be defined as an environment in which computers and similar devices communicate with one another. Hence, Raymond's arguments, which suggest that the Internet cannot be considered a global common due to the lack of uniform control mechanisms and the presence of strict state regulations, highlight a crucial distinction. While the Internet's governance may vary significantly across different national

¹² Mbanaso and Dandaura, "The Cyberspace: Redefining A New World."

¹³ International Telecommunication Union, "Individuals using the Internet," ITU-D ICT Statistics, accessed December 2, 2023, <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

¹⁴ Charlotte Hess, "Untangling the Web: The Internet as a Commons," (paper presented at the Workshop in Political Theory and Policy Analysis, Indiana University, Bloomington, March 1996), https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/327/Untangling_the_Web96.pdf?sequence=1&isAllowed=y.

¹⁵ Lawrence Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (New York: Random House, 2001), 14.

¹⁶ Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, 2013, 53-64, <http://www.jstor.org/stable/43134322>.



contexts, cyberspace, as a more pervasive and extensive domain, transcends these limitations. This broader perspective suggests that cyberspace, unlike the Internet alone, could potentially function as a global common, given its ubiquitous influence and integral role in global communication and information exchange.

A comparative analysis reveals both commonalities and differences between cyberspace and traditional global commons. Cyberspace aligns with the generic definition of global commons - namely, not being the exclusive domain of any single nation or entity and serving as a shared resource for the greater good of humanity. However, it possesses unique characteristics that set it apart from other global commons.

Unlike other global commons, which are naturally occurring phenomena, cyberspace is a human-made construct predominantly owned and managed by the private sector. While traditional global commons facilitate the transfer of people and materials, cyberspace primarily enables the transfer of information and data. Additionally, traditional global commons have tangible and physical dimensions, whereas cyberspace is difficult to measure and quantify. Modern technologies such as cloud computing, big data, the deep web, and the dark web contribute to the potentially infinite nature of this virtual domain.

The terms 'surfing' and 'browsing' are attempts to relate the abstract and highly technical activity of navigating cyberspace to the material world familiar in daily life. These analogies underscore the inherent challenge in conceptualising cyberspace.

Traditional global commons are accessible to all, but exploiting these domains often requires significant human, fiscal, and scientific resources, placing them beyond the reach of ordinary individuals and even some smaller nations. In contrast, cyberspace is readily accessible and exploitable by ordinary people with a computer and necessary software.

Over time, independent thinkers like John P. Barlow¹⁷ and various governments have increasingly embraced the notion of cyberspace as a global common. While previous discussions highlighted its unique characteristics, it is equally important to recognise the similarities and common features with other global commons. Like outer space,

¹⁷ John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, February 8, 1996, <https://www.eff.org/cyberspace-independence>.

cyberspace is ubiquitous and impractical to restrict access to. The Internet, the foundational element of cyberspace, is built on global, non-proprietary standards that anyone can adopt. Similar to the high seas, it is in the interest of all nations to facilitate free access and unimpeded flow of data and services across cyberspace. Moreover, like all other global commons, cyberspace holds immense economic value and virtually unlimited potential for human benefit.

Cyberspace is also as susceptible to misuse as any other global commons. Similar to piracy at high seas, hackers and non-state actors exist in cyberspace and pose a great threat. When such activities are carried out by states and state-sponsored actors, this becomes a potential matter of national security for the target nations.

Analysis reveals that cyberspace indeed possesses all the qualifying characteristics of a global common: the lack of single-state ownership, accessibility, and shared benefits for humanity.¹⁸ These attributes far outweigh the arguments against its classification as a global common. The question of why cyberspace is not globally recognised and governed like other commons warrants further study.

Cyberspace and Global Governance

At present, global governance of cyberspace or the internet does not exist at an international scale or forum. Documented treaties or pacts are a mosaic of non-related and non-global attempts to regulate the activities within cyberspace. These are between limited states or private sector entities across the world and mainly focused on technical aspects of the internet and internet-based services. The US-Based, non-profit organisation called the Internet Corporation for Assigned Names and Numbers (ICANN), is responsible for assigning unique domain names and IP addresses across the globe.¹⁹ The World Wide Web Consortium (W3C) is also a non-profit organisation mainly responsible for international standards for the internet. Its members include

¹⁸ Michael John V. Mago and Ma. Anna Katerina C. Fulgencio, *Global Governance in Cyberspace: Delineating Obligations in the Cyber Context* (paper, CIRSS Commentaries, Center for International Relations and Strategic Studies, Washington, D.C., April 2023), 3, https://fsi.gov.ph/wp-content/uploads/2023/05/April-2023_Mago_Fulgencio.pdf.

¹⁹ Internet Corporation for Assigned Names and Numbers, "ICANN for Beginners," accessed June 24, 2024, <https://www.icann.org/en/beginners>.

businesses, other non-profit organisations, individuals, state entities, and universities.²⁰

Two examples of limited international cooperation in cyberspace governance can be cited. The first is the EU's 'Convention on Cybercrime', also known as the 'Budapest Convention on Cybercrime'.²¹ Its membership is primarily limited to European countries, lacking broader global participation and acceptance. The second example is the 'African Union Convention on Cyber Security and Personal Data Protection.'²² This convention is also restricted to regional participation and does not form part of a global regime.

At the national level, nearly all nations have enacted local laws to prevent cybercrimes and other criminal activities in cyberspace. The nuance that distinguishes cyberspace from other global commons is the absence of a global or widely accepted international legal framework to govern it.

Cyberspace and State Sovereignty

The preceding comparison compels a deeper consideration of the notion of state sovereignty in cyberspace. This concept is grounded in the fact that cyberspace operates on physical infrastructure - whether wired or wireless - located within defined national boundaries. Consequently, all communication devices and networks owned by individuals or organisations fall under the jurisdiction of specific national laws. This suggests that states possess the capability to regulate and manage cyberspace in alignment with their particular interests. The examples of China and Iran illustrate how states can exert control over cyberspace to enforce their policies and priorities.

A critical analysis of the controls imposed by states reveals several negative implications, suggesting that these measures are not ideal solutions. Firstly, these controls can be argued to deny individuals the right to access global resources available in cyberspace, thus constituting a breach of individual freedom. Secondly, such measures can lead to a form of isolation from the broader global cyber community, hindering the free exchange of information and ideas. Thirdly, these

²⁰ World Wide Web Consortium (W3C) "About Us," accessed June 24, 2024, <https://www.w3.org/about/>.

²¹ Council of Europe, "Convention on Cybercrime," European Treaty Series 185, Budapest, November 21, 2001, <https://rm.coe.int/1680081561>.

²² African Union, "African Union Convention on Cyber Security and Personal Data Protection," EX.CL/846(XXV), Malabo, June 27, 2014, http://www.opennetafrica.org/?wpfb_dl=4.

mechanisms are often technically imperfect and require significant fiscal resources to implement. The fiscal penalties include governance costs and economic implications for local firms engaged in international trade. The Sino-Russian bloc, which advocates for strict cyberspace sovereignty, exemplifies this approach with tighter state controls over the Internet and related technologies in these countries.

A Global Cyberspace Governance Regime

Global governance of cyberspace has been a topic of discussion for the last few decades. Notably, despite the absence of single-party ownership, there are various groups and international entities moving toward a potential governance regime. These bodies include corporations, governments, private entities, civil society, and international actors. Research scholar Haekal Al Asyari discusses this issue extensively, arguing that the Common Heritage of Mankind (CHM) principles can be applied to cyberspace. He advocates for the establishment of an international body to control and regulate cyberspace, ensuring equitable access and management of this critical global resource.²³

On the international scale, various efforts indicate a move towards consensus on the global understanding and eventual governance of cyberspace. In 2004, under the auspices of the United Nations, a Group of Governmental Experts (GGE) was formed, comprising representatives and subject matter experts from multiple countries. The GGE's report, particularly the one in 2013, made several significant conclusions and recommendations. One key acceptance was that 'State sovereignty and the international norms and principles that flow from sovereignty apply to State conduct in cyberspace.' This acknowledges that a state has jurisdiction over cyber infrastructure within its territory. However, it also highlighted that 'States must meet their international obligations regarding internationally wrongful acts attributable to them' and that states must not use proxies to commit internationally wrongful acts.²⁴ This UN commissioned report indicates that there has existed a general understanding

²³ Haekal Al Asyari, "Cyberspace as a Common Heritage of Mankind: Governing Normative Limitations of the Internet by Virtue of International Law," *Acta Universitatis Carolinae Iuridica (AUC Iuridica)* 69, no. 4, (2023): 211-228, https://karolinum.cz/data/clanek/12015/Iurid_69_4_0211.pdf.

²⁴ United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General," A/68/98, June 24, 2013, 2, <https://undocs.org/A/68/98>.



that some international laws are applicable in cyberspace. However, the enforcement mechanism for its practical application remains missing.

A similar exercise was undertaken by NATO members through the Cooperative Cyber Defence Centre of Excellence (CCDCOE). NATO arranged for a group of experts to examine the issue further, resulting in the development of the 'Tallinn Manual on the International Law Applicable to Cyber Warfare.' This group worked for three years to produce the first edition of the Tallinn Manual, which was published in 2013. The second edition, known as Tallinn Manual 2.0, was published in 2017. The first edition contained 95 rules proposed by the experts, aimed at providing guidelines on how the legal framework can be applied to nation-states in the cyber domain.²⁵ Tallinn Manual 2.0 aimed to define processes and clarify controversial issues. It concluded that the manual serves as a valuable starting point for international engagement. However, it also highlighted areas of disagreement and ambiguity. The bottom line though was that it stressed that a state-based legal framework is necessary to address cyberspace governance effectively.²⁶

The next significant step was the GGE report of 2015 which took into consideration existing and emerging threats, risks and vulnerabilities, and built upon the assessments and recommendations contained in the 2013 report. This one moved closer to recognising the need for a UN-sponsored regime for the governance of cyberspace under a legal framework. It clearly noted that other already accepted and established legal principles governing armed conflict, principles of humanity, necessity, proportionality, and distinction exist under a legal framework. The report however, did not elaborate on the application of these principles to cyber activities. Most importantly, it recognised that 'a common understanding on how international law applies to State use of ICTs [cyberspace] are important for promoting an open, secure, stable, accessible and peaceful ICT [cyber] environment.'²⁷

²⁵ Lauren M. Cherry and Peter P. Pascucci, "International Law in Cyberspace," *American Bar Association*, January 27, 2023, https://www.americanbar.org/groups/law_national_security/publications/aba-standing-committee-on-law-and-national-security-60-th-anniversary-an-anthology/international-law-in-cyberspace/.

²⁶ Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 735-778. <https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf>.

²⁷ United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the

In 2018, the UNGA passed a resolution to reconstitute the GGE in 2019, tasking it with continuing to study the subject to promote common understandings and effective implementation of a legal framework. The GGE submitted its report, which was adopted by participating states on 13 July 2021.²⁸ The UNGA Resolution had called for all invited states to submit their views on how international law applies to state cyber activities. Consequently, the GGE report is a compilation of the participating states' views and submissions on the topic. It offers a detailed and insightful perspective on how states interpret these issues and apply international law, particularly through the lens of state security.

During the same period, under a Russian initiative,²⁹ the UNGA passed resolution 75/240 to form an 'Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025'. Its mandate is to establish rules and norms concerning states' behaviour in the use of information technologies. So far, it has had eight substantive sessions – the most recent one in March 2024 to be followed by one in July.³⁰ Consequently, two parallel processes have been initiated, indicating a power contestation and bloc-wise approach to the governance and law of cyberspace. This dual-track effort highlights the complexities and geopolitical dimensions of international cyber security governance.

The discussion on state sovereignty and cyberspace governance leads to several conclusions and raises further questions regarding the complexities and challenges of achieving a global consensus on cyberspace governance:

Secretary-General," A/70/174, July 22, 2015, 13,
<https://digitallibrary.un.org/record/799853?ln=en&v=pdf>.

²⁸ United Nations General Assembly, "Official Compendium of Voluntary National Contributions on the Topic of How International Law applies to the Use of Information and Communications Technologies by States submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266," A/76/136, July 13, 2021, https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf.

²⁹ United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the First Committee," 75/394, November 16, 2020, <https://documents.un.org/doc/undoc/gen/n20/316/62/pdf/n2031662.pdf?token=hVSgiZu6EICroc iU6X&fe=true>.

³⁰ United Nations Office for Disarmament Affairs, "Open-ended Working Group on Security of and in the Use of Information and Communications Technologies," accessed June 24, 2024, <https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021>.



- i. Cyber sovereignty³¹ is increasingly acknowledged as a fundamental principle in discussions on international cyberspace governance. This recognition implies that each state asserts its right to manage and control the internet and cyber activities within its territory.
- ii. There is a general trend toward developing regional and international frameworks aimed at regulating state behaviour in cyberspace. These efforts reflect the need for coordinated responses and shared norms to address cyber threats and ensure the security and stability of cyberspace.
- iii. The UN's inability to enact specific protocols for cyberspace governance is largely due to differing views among states on how to approach the global governance of cyberspace. These differences prevent the formulation of a unified global framework.

The question of why nations do not share a unified view on cyberspace governance mirrors historical difficulties in reaching consensus on other global commons, such as maritime or environmental regulations. However, international laws have eventually been established in these areas, despite initial disagreements.

So, what makes cyberspace different?

Besides the fact that nation-states view this issue through the lens of national security, leading to protective and sometimes secretive policies regarding their cyber infrastructure and capabilities, cyberspace's distinct challenges stem from several other factors:

- The **digital economy** is deeply integrated with cyberspace, adding layers of economic interests that complicate international negotiations.
- Differences in **technical capabilities and infrastructure** among countries create disparities in how states can engage with and benefit from global cyberspace regulations.
- In cyberspace, the **range of stakeholders** is broader than in any other global common. This includes states, corporations, non-state actors, organisations, and individuals, each with their own interests and objectives. This diversity

³¹ United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General," A/70/174.

complicates consensus-building as each group has unique priorities and concerns.

- Cyberspace is defined by **rapid technological advancements**, making it difficult to establish long-lasting norms that adapt to continuous changes.
- States prioritise their **sovereignty**, leading to a reluctance to relinquish control over cyberspace to international agreements. This prioritisation often results in a protective stance toward national cyber infrastructure and data regulations.
- Stark differences in how **fundamental principles** such as privacy, cyber security, and freedom of expression are valued and regulated further obscure efforts to establish a common international framework. These principles are often interpreted differently across legal and cultural contexts, making universal agreements challenging.
- The **attribution of cyber-attacks** is notoriously difficult, which muddles accountability and response strategies. The militarisation of cyberspace by some states also adds a layer of security concerns that can impede cooperative governance efforts.
- The **digital divide** between countries, where some nations have advanced technological capabilities and others do not, impacts how effectively countries can participate in and benefit from global cyberspace regulations.

The diversity of actors and the complex issues previously discussed introduce significant challenges to international law and arbitration.³² Despite these challenges, there is a growing trend and ongoing discussions within the international community to advocate for the application of customary international law as the foundation for cyberspace governance.³³ This movement underscores a collective effort to standardise the legal framework across nations to better manage and secure cyberspace.

³² Al Asyari, "Cyberspace as a Common Heritage of Mankind," 222.

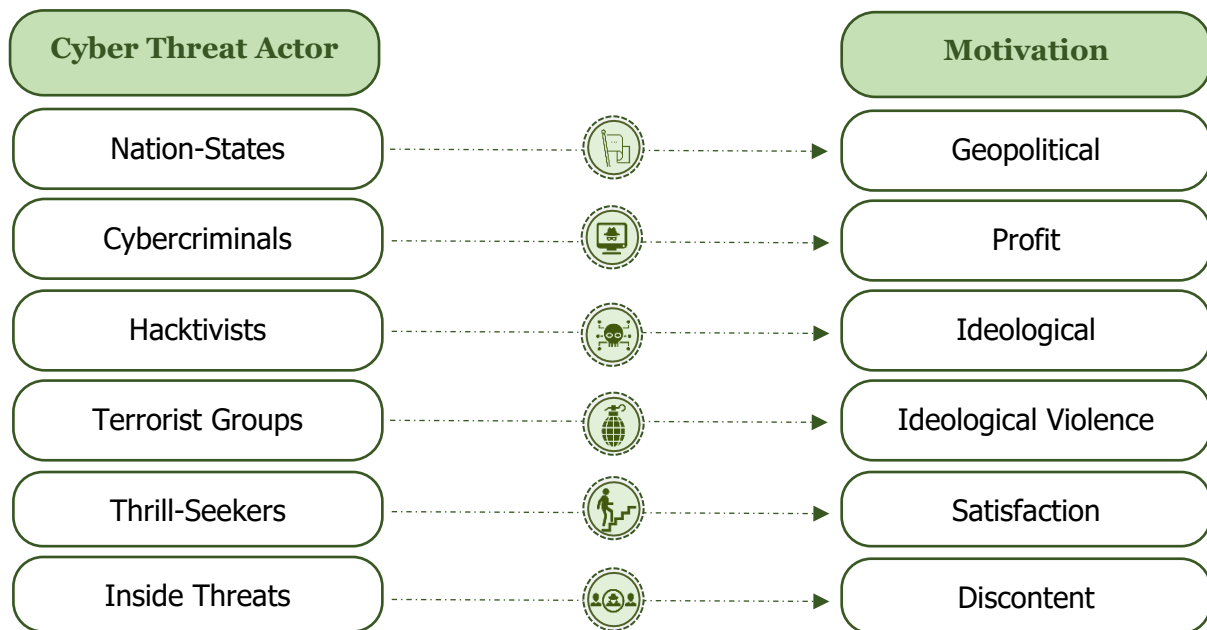
³³ Wouter Werner, *Repetition and International Law* (Cambridge: Cambridge University Press, 2022), 15.

Threats

If security concerns prevent all nation-states from agreeing on global governance of cyberspace, it is prudent to examine how various nations perceive threats originating from this domain. With the exponential growth of cyberspace, dependencies at international, national, organisational, and personal levels have also significantly increased, often beyond control. Concurrently, the number of actors eager to exploit these dependencies has risen. These actors range from governments and state-sponsored groups to individual cybercriminals, each with diverse motivations. While some, like nation-states, may engage in cyber activities to steal intellectual property, others, such as cybercriminals, often seek financial gain. Additional motivational factors include the propagation of ideological beliefs or personal vendettas. This complex array of motivations and actors underscores the challenges in forming a unified global approach to cyber governance.

In today's digital era, cyber-attacks can have profound impacts. Even small groups with limited resources are capable of damaging the critical or strategic systems of a victim state. This issue is further exacerbated as nation-states increasingly rely on cyber-based infrastructure and e-commerce. The variability in how nations perceive and define threats originating from cyberspace complicates international efforts to establish common defensive measures. An illustrative example of threat categorisation is provided by the Canadian Communications Security Establishment, which outlines a range of cyber threats and identifies the diverse actors involved in such activities. This approach helps in understanding the multi-faceted nature of cyber threats and aids in tailoring national security measures accordingly (Figure 1):

Figure 1: Cyber Threat Categorisation



Source: Communications Security Establishment and Canadian Centre for Cyber Security, *An Introduction to the Cyber Threat Environment 2023-2024* (Ottawa, 2022), 2, <https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf>.

Similar threat identification frameworks have been adopted by other countries, including the US³⁴ and the United Kingdom (UK).³⁵ This indicates that it has become necessary for all states to understand and prioritise cyber security as crucial to national security.

Using Buzan’s model of national security,³⁶ Forrest Hare applied this theoretical framework in the context of cyber security. He posited that regardless of a state’s sociopolitical cohesion, all states are vulnerable to cyber threats. The specific nature of the targets may vary from one state to another, reflecting the differing strategic interests and infrastructural dependencies across nations. This perspective reveals that the threat of cyberattacks is a universal concern that transcends traditional geopolitical boundaries and requires a coordinated global response to effectively manage and mitigate.³⁷

³⁴ National Counterintelligence and Security Center, “Cyber Security,” Office of the Director of National Intelligence, accessed March 24, 2024, <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-cyber-security>.

³⁵ Amber Keegan and Lydia Harriss, “States’ Use of Cyber Operations (paper, Research Briefing Number 684, UK Parliament Post, October 27, 2022), <https://post.parliament.uk/research-briefings/post-pn-0684>.

³⁶ Barry Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era* (Chapel Hill, N.C.: University of North Carolina Press, 1983), 20.

³⁷ Forrest Hare, “The Cyber Threat to National Security: Why Can’t We Agree,” (paper presented at the Conference on Cyber Conflict, Tallinn, 2010), 211-225,



Who would Govern Cyberspace and Great Power Contestation

When discussing global governance of cyberspace, it is crucial to consider the international cybersecurity environment through the prism of great power contestation. The U.S. State Department, in its 'International Cyberspace and Digital Policy' released on May 6, 2024, acknowledged the cyber threats to national security and outlines strategies to mitigate these threats. Notably, the policy document explicitly identifies China, Russia, and North Korea as the principal cyber threats to US national security. This stance underscores the geopolitical dimensions of cyberspace, where state actions in the digital realm are closely intertwined with broader national security strategies and international relations.³⁸

The Chinese approach to cyberspace governance differs significantly from that of the US, influenced by both historical strategy and contemporary events. Concerns heightened by the Arab Spring in 2011, which demonstrated the powerful role social media can play in political mobilisation, have shaped China's stringent control measures over the internet. This concern was further reinforced in 2013 after the Egyptian military coup, which was also influenced by social media dynamics. As a response, China has established what is widely known as the 'Great Firewall of China.' Through this sophisticated technical system, China exercises strict control over internet access, blocking and restricting public access to certain internet resources and social media networks. The overarching goal is to modify public behaviour in cyberspace, driven by the fear of investigation and subsequent legal repercussions. This strategy is part of a broader legal framework designed to maintain state control and prevent the kind of social unrest seen in other parts of the world.³⁹

The contrasting stances of major powers like the US and China highlight a fundamental issue: each perceives a real and imminent threat from the other in terms of national security, which can easily escalate into the realm of cyberwar. This perception significantly hinders the global community, particularly great powers, from reaching a

<https://ccdcoe.org/uploads/2018/10/Hare-The-Cyber-Threat-to-National-Security-Why-Cant-We-Agree.pdf>.

³⁸ U.S. Department of State, *United States International Cyberspace & Digital Policy Strategy*, report (Washington, D.C., May 6, 2024), <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/#:~:text=The%20United%20States%20seeks%20to,the%20exercise%20of%20human%20rights%2C>.

³⁹ Jinghan Zeng, Tim Stevens and Yaru Chen, "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty,'" *Politics & Policy* 45, no. 3 (June 2017):432-464, <https://onlinelibrary.wiley.com/doi/abs/10.1111/polp.12202>.

consensus on establishing and applying international law in cyberspace. The fear of vulnerability and the strategic advantage that cyber capabilities offer mean that nations are cautious about limiting their own options in cyberspace through binding international agreements. This impasse underscores the complexities of cyber diplomacy where national security concerns directly conflict with the need for global cooperation in cybersecurity and cyber governance.⁴⁰

The concept of cyberwar has been a subject of scholarly debate since the early 1990s.⁴¹ Pioneering thinkers like John Arquilla and David Ronfeldt were among the first to argue that cyberwar is a real possibility, suggesting that conflicts in cyberspace could mirror traditional warfare in their impact and organisation. In contrast, Thomas Rid posited that cyber activities such as cyberattacks do not meet the traditional definitions of war. Instead, Rid categorises them as acts of 'subversion, espionage, and sabotage.'⁴² While the exact scale and possible of cyberwarfare is difficult to predict, contestation and offensive actions remain a firm reality.

Analysis

When analysing the issue of cyberspace governance, it is crucial to consider the diverse array of stakeholders involved in what might be termed the 'great game' of cyberspace. These stakeholders, or 'players,' each wield different levels of leverage and have their own distinct 'interests' or stakes in the governance of cyberspace (Table 1):

⁴⁰ Eric Rosenbach and Shu Min Chong, "Governing Cyberspace: State Control vs. The Multistakeholder Model," (paper, Belfer Center for Science and International Affairs, Harvard Kennedy School), <https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model>.

⁴¹ John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141-165, reprinted in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt, RAND Corporation, 1997, <https://www.rand.org/pubs/reprints/RP223.html>.

⁴² Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 5-32, <https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939>.



Table 1: Cyberspace Stakeholders

Players	Leverage	Interests
Great Powers	High	Power
Developed Nations	Medium	Power Sharing
Developing Nations	Low	Security
International Organisations	High	Standards
Tech Giants	High	Economic
Civil Societies	Low	Freedom

Source: Author's own.

The interplay of players, leverage and interests makes the issue of global cyberspace governance extremely complex. The US and Chinese stances, though briefly discussed earlier, share certain similarities which include:

- **Safeguarding critical infrastructure and strategic capabilities:** Both states are focused on the importance of protecting their critical systems from cyber threats.
- **Ensuring the safety of critical data:** This involves measures to protect sensitive information from cyber espionage and data breaches.
- **Enhancing technological prowess in cyberspace:** Each aims to advance its technological capabilities to maintain or gain a strategic advantage in cyberspace.

Despite these similarities, a stark clash of interests over the governance of cyberspace prevents the great powers from reaching a consensus. Developed nations, including the EU and the UK, also prioritise cyber sovereignty but lack sufficient influence to sway global opinions or achieve a consensus. Their efforts are more focused on regional cooperation and establishing mutually acceptable norms within their spheres, as evidenced by initiatives like the Tallinn Manual, which seeks to clarify international law as it applies to cyber warfare and cyber operations.

As discussed, international organisations, particularly the UN, have also been actively making efforts to mobilise all nation-states toward a universally accepted solution for

cyberspace governance through initiatives such as GGEs and the OEWG. However, the contrasting roles and interests of major tech giants introduce a completely different set of complexities. Companies like Microsoft, Google, and Apple wield significant leverage due to their technological monopolies. Their economic interests often prioritise less regulated cyber environments, which they argue promote innovation and economic growth, over the benefits of a controlled cyberspace, whether nationally or globally.

This stance is exemplified by a notable incident involving Yahoo in the year 2000. Yahoo started an online auction of Nazi memorabilia, which, while legal in the US, violated French laws against the sale of items that could incite racial hatred. A case, filed by the French-based International League against Racism and Anti-Semitism (LICRA), led to a legal battle in France. The Tribunal de Grande Instance de Paris ruled against Yahoo, ordering the company to block access to the auction from France and imposing a fine for non-compliance. This legal outcome underscores the difficulties tech companies face when national laws clash with the borderless nature of the Internet. Heather Killen, a VP at Yahoo, encapsulated this challenge, 'It is very difficult to do business if you have to wake up every day and say 'OK, whose laws I follow? We have many countries and many laws but just one Internet.'⁴³

Civil societies often wield minimal leverage in the international regulation of cyberspace. While advocating for freedoms such as expression and access remains a common goal, the influence of civil societies can vary significantly by region. In developed countries, these organisations may have a tangible impact on shaping national laws. However, in developing countries or those under authoritarian regimes, civil societies frequently find themselves with limited ability to influence policy at the national level. Such disparity highlights the challenges faced by civil society groups in participating meaningfully in discussions and decision-making processes related to cyber governance on both a national and global scale.

This scenario underscores a fragmented approach to global cyberspace governance, where regional alignments and agreements, such as those guided by the Tallinn

⁴³ Raphael Cohen-Almagor, "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications," *Journal of Business Ethics* 106, no. 3 (July, 2015): 353-365.



Manual, play critical roles but fall short of establishing a universal framework accepted by all key players.

Future Outlook

As seen with UNCLOS, while it is globally recognised, numerous conflicts within this regime persist, as illustrated by disputes in the South China Sea and the Bab-El-Mandab in the Red Sea. These regions highlight how states and non-state actors sometimes disregard the binding international law governing open seas. Conversely, when economic and trade interests are at stake, particularly in combating piracy, there is a notable unified resolve among states, demonstrating a selective adherence to international norms based on collective economic security interests.

This pattern mirrors the challenges and potentials in cyberspace governance. The Budapest Convention and the African Union's initiatives on cyber security reflect a growing recognition among states of the need for governance through mutually agreed norms in cyberspace. However, these efforts remain confined to multilateral or regional frameworks. Globally, initiatives like the UN's Group of Governmental Experts (GGE) signify international engagement, yet these have not culminated in practical and binding global solutions. This dichotomy underscores the complex landscape of international relations where strategic interests often dictate the level of commitment to and compliance with global norms.

Over the last two decades, scholarly discussions on models of global governance in cyberspace have been robust, yet they have also been marked by lack of consensus. Joseph S. Nye Jr, a prominent scholar in this field, has contributed significantly to this debate by proposing a multi-stakeholder model of cyberspace governance.⁴⁴ This model acknowledges the complexity of international relations and the diverse interests at play. In his argument regarding a 'Regime Complex,' Nye underlines the challenges in establishing a single, unified governance framework for cyberspace. He argues that due to the varied interests and powers of different stakeholders, it is unlikely that a single overarching regime will emerge in the foreseeable future.

⁴⁴ Joseph S. Nye Jr, "The Regime Complex for Managing Global Cyber Activities," (paper, Series No. 1, Centre for International Governance Innovation and the Royal Institute for International Affairs, Ontario and London, 2014), https://www.cigionline.org/static/documents/gcig_paper_no1.pdf.

On the surface, the easiest and most logical solution to the problem, then, perhaps lies in looking at the use of cyberspace for activities against another state as equivalent to the use of military force. Or does it?

While recognising cyber operations akin to the use of military force might seem straightforward, given existing international laws that prohibit the use of force by one state against another, this approach is fraught with complexities.

The primary challenge involves issues of 'Deniability and Attribution.' Unlike conventional or military uses of force, cyberattacks can be executed in ways that leave no clear physical or digital trace. For example, if country A launches a cyberattack against country B using the digital infrastructure of country C, without C's knowledge or involvement, the attack remains deniable, and attributing it definitively to country A becomes problematic. Secondly, the purposes of cyberattacks vary widely, ranging from theft of sensitive data to crippling a nation's strategic capabilities. This variability makes it challenging to define what constitutes an 'act of war' in the cyber realm. Furthermore, the rise of Artificial Intelligence and autonomous weapons adds another layer of complexity. These technologies can obscure the source and intent of cyber operations even further, complicating the attribution process and the application of international law.

Thus, while equating certain cyber operations with military actions could leverage existing legal frameworks to govern state behaviour, the unique characteristics of cyber warfare demand nuanced and adaptable legal and diplomatic responses.

Predicting the future of international cyber governance is difficult due to the accelerated pace of technological advancements, conflicting national interests, great power contestation, and a growing realisation of threats to national security. It is reasonable to anticipate that rather than a single entity or regime exercising centralised control over cyberspace, there will likely be an increase in stricter national policies and regimes aimed at securing individual cyber sovereignty. In this scenario, national cyberspace could be treated similar to national geographical boundaries.

The recent US 'National Cyber Security Strategy'⁴⁵ and 'International Cyberspace & Digital Policy Strategy'⁴⁶ indicate that the battle lines are being drawn.

Any approach towards an international agreement would necessitate the formulation of policies and Confidence Building Measures (CBMs) by all stakeholders to facilitate a global consensus. Therefore, it is essential for the United Nations to continue its efforts with added vigour to foster a multilateral agreement that addresses the complexities of cyberspace. Concurrently, states must demonstrate a willingness to actively participate in the development of rules and regulations concerning cyberspace. Simultaneously, nation-states would have to increasingly rely on domestically developed technical, operational, and procedural solutions to safeguard their individual cyberspace boundaries. This two-pronged approach - global cooperation enhanced by robust local measures - reflects the multifaceted nature of cyberspace governance, where international norms must be complemented by strong national cybersecurity strategies to create a secure, stable, and resilient digital environment.

⁴⁵ The White House, *National Cyber Security Strategy 2023* (Washington, D.C., 2023), <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

⁴⁶ U.S. Department of State, *United States International Cyberspace & Digital Policy Strategy*.



ABOUT THE AUTHOR

Air Marshal Zahid Mehmood (Retd)

joined the Centre for Aerospace & Security Studies, Islamabad as Director in November 2023. A graduate of National Defence University and Air War College, he has 36 years' experience of military aviation as a fighter pilot in the Pakistan Air Force (PAF). During his service with the PAF, he has held various Command and Staff appointments including Assistant Chief of Air Staff (Plans), Director General C4I, Deputy Chief of Air Staff Personnel and Vice Chief of Air Staff. He holds Master's Degrees in Strategic Studies and Defence & Strategic Studies. An alumnus of the Harvard Kennedy School for National and International Security (USA), his areas of expertise include National Security with emphasis on traditional security threats and response options as well as cybersecurity. He lectures regularly at Pakistan's National Defence University and Air War College on related subjects. He was awarded Hilal-i-Imtiaz (Military) for his services to the PAF.

ABOUT CASS

The Centre for Aerospace & Security Studies (CASS), Islamabad, was established in 2018 to engage with policymakers and inform the public on issues related to aerospace and security from an independent, non-partisan and future-centric analytical lens. The Centre produces information through evidence-based research to exert national, regional and global impact on issues of airpower, emerging technologies and security.

VISION

To serve as a thought leader in the aerospace and security domains globally, providing thinkers and policymakers with independent, comprehensive and multifaceted insight on aerospace and security issues.

MISSION

To provide independent insight and analysis on aerospace and international security issues, of both an immediate and long-term concern; and to inform the discourse of policymakers, academics, and practitioners through a diverse range of detailed research outputs disseminated through both direct and indirect engagement on a regular basis.

CORE AREAS OF RESEARCH

Aerospace

Emerging Technologies

Security



Strategic Foresight



**CENTRE FOR
AEROSPACE & SECURITY
STUDIES, ISLAMABAD**
Independence. Analytical Rigour. Foresight

 Old Airport Road, Islamabad, Pakistan
 cass.thinkers@casstt.com
 Centre for Aerospace & Security Studies

 +92 051 5405011
 www.casstt.com
 [cassthinkers](https://www.instagram.com/cassthinkers)

 [@CassThinkers](https://twitter.com/CassThinkers)
 [cass.thinkers](https://www.facebook.com/cass.thinkers)