FOREWORD

The power of the Internet is real. It is synonymous with freedom of expression, it is an information powerhouse, and it has a tremendous ability to influence and direct narratives. We tend to think of cyberspace as being a common and non-invasive medium for all individuals and governments, but that is not true. It can be harnessed to generate enormous destructive power, whether it is targeted at critical physical infrastructure or at the minds of the population and its leadership. It is a perfect weapon in the hands of those who can control and influence the data which resides in the cyberspace.

Pavithran Rajan was an Intelligence Corps officer in the Indian Army. He therefore has a unique understanding of the types of threats facing the nation. He has studied InfoWar in great detail, and after his retirement, worked tirelessly with academia, industry and the government to recommend ways in which we can strengthen our policies and infrastructure to deal with the emerging cyber challenges. In a well-argued essay, “The Fallacy of Cyber Commons”, Rajan brings out the domination of the United States of America on the cyber commons. Armed with the power that this domination wields, it would be foolish for anyone to expect America not to exploit this strength. With its superiority in technology and a major world share in hardware and software industry, USA is unlikely to loosen its grip.

The Global Cyber Vulnerability Report, published in Dec 2015, found that India is the most cyber-vulnerable country in the World, with the highest rate of attacks per machine. China and Russia also figure in the top five vulnerable countries. What clearly distinguishes these two countries from India is the cogent
and visible steps being taken by them to reduce their vulnerability.

An understanding of this vital issue is important as India looks to craft its future response to cyber threats. It sometime defies comprehension that we continue to insist on using foreign hardware and software in our critical areas. Fledgling attempts at introducing Open Source indigenous solutions in the government have faced enormous resistance from senior civil and military bureaucracies. To be generous, this can perhaps be put down to a lack of understanding of the strategic dimension of cyberspace, by a generation, which saw the first TV set only in its teens.

The strategic significance of data in the information age, and its impact on various spheres of human activities is still little understood in official circles of India. Here too the USA has evolved a strategy to ensure that the largest depositories of data are under their control through promotion of US MNCs. These ever increasing data depositories are only now beginning to be mined by Artificial Intelligence and could result in full spectrum domination of the globe, the likes of which have never been witnessed in history. Rapid policy changes to adapt and encourage private ICT entrepreneurship and a privacy law to look after the interests of its citizens are the need of the hour.

It is for this reason that Rajan’s paper is important. In very simple terms, it brings out the need for a large and developing country like India to create its own indigenous ICT solutions in order to protect its vital interests. Anything less will put us at grave risk. It is not an impossible task. We have the people and ability to make it happen. The impetus will have to and must come from the government.

Lt Gen Deependra Singh Hooda, PVSM, UYSM, AVSM, VSM** (Retd)
The Fallacy Of The Cyber Commons

by

Pavithran Rajan
Introduction

The global commons have been defined as those areas that are not under the control of a particular state, but are open for use by states, organizations, and individuals worldwide. They have also been described as the “fabric or connective tissue of the international system,” and include the sea, air, space, and cyberspace domains. The term “commons” was originally coined by Admiral Alfred Thayer Mahan in his seminal study entitled, *The Influence of Sea Power Upon History.*

Admiral Alfred Thayer Mahan

Mahan revolutionized the concept of commerce and warcraft through his analysis of military control of the seas. Mahan reviewed the role of sea power in the emergence and growth of the British Empire. He identified several narrow passages or strategic “chokepoints,” the control of which contributed to Great Britain’s command of the seas. Mahan drew attention to the economic benefits gained from control of such passageways through the creation of trade routes and the consequent power a state could reap by dominating seaborne commerce. Mahan also foresaw as early as 1901 the fundamental geopolitical
realities of the Cold War that emerged from the ashes of the first two world wars. In *The Problem of Asia*, Mahan urged world leaders to “glance at the map” of Asia and note “the vast, uninterrupted mass of the Russian Empire, stretching without a break from the meridian of western Asia Minor, until to the eastward it overpasses that of Japan.” He envisioned a Russia that would have to be contained by an alliance of the United States, Great Britain, France, Germany, and Japan, which is precisely what happened between 1945 and 1991 and continues to this day.4

Mahan also recognized the potential of China and foresaw a time when the United States would need to be concerned with China’s rise. Mahan wrote a letter in 1893 to the editor of the *New York Times* in which he urged the annexation of Hawaii by USA as a necessary first step to exercise control of the North Pacific. Mahan also foresaw a struggle for power in the area of Central Asia he called the “debatable and debated ground,” and identified the “immense latent force” of China as a potential geopolitical rival. Mahan knew that Western science and technology would, at some point, be globalized and wrote that under such circumstances “it is difficult to contemplate with equanimity such a vast mass as the four hundred millions of China concentrated into one effective political organization, equipped with modern appliances, and cooped within a territory already narrow for it.” 5

In 2016 if Mahan had been alive, he would have also added India, home to 1.3 billion, dominating the sea-lanes of communication of the Indian Ocean with a rapidly growing economy, having a huge population dividend and a talented human resource, as a future threat. The Indian elite does not see these realities and are preoccupied with the internal politics of a cacophonic democracy. They profess their peaceful intentions to the world and believe that their civilization is inherently a peaceful one as they have rarely ventured out of the Subcontinent, not realizing that it has more to do with the
geography of its neighborhood than that of any cultural or civilisational reasons. They have a vague idea of the great potential of their ancient nation but do not realize the dangers that, apprehensions of others to their latent potential are inherently the source of strategic threats to the Indian nation. Alfred Thayer Mahan was a visionary who actually saw naval strategy as a construct for both a political and economic system. The 21st century now has a different ocean with much larger potential – Cyberspace.

Global Commons

![Image of Barry Posen](image)

Barry Posen

In 2003, Barry Posen a Ford International Professor of Political Science at MIT and the director of MIT’s Security Studies Program wrote a landmark piece on the defense and security benefits of having unchallenged freedom of operation in the commons entitled, *Command of the Commons: The Military Foundation of U.S. Hegemony*. Posen argued that the ability to dominate these shared domains serves as the foundation of the leadership role that the United States holds in the international system. He stated, “Command of the commons is the key enabler of the U.S. global power position. It allows the United States to exploit more fully other sources of power, including
its own economic and military might as well as the economic and military might of its allies. Command of the commons also helps the United States to weaken its adversaries, by restricting their access to economic, military, and political assistance”. Posen’s work on this topic brought to the forefront the role that the global commons play as a key enabler of U.S. defense, national security and economic strategies. 6

As the 2010 U.S. Department of Defense’s Quadrennial Defense Review Report states, “Global security and prosperity are contingent on the free flow of goods shipped by air or sea, as well as information transmitted under the ocean or through space.” 7 Access to the global commons enables these flows, in turn promoting both international prosperity and stability. The ability to control this access is the key to coercive diplomacy in the world order crafted by the US and its Western allies and the ability of other nations and their armed forces to ensure the unrestricted access to the global commons in varying degrees is what determines the pecking order of global power.

Thus a commons can be defined as: -

* A space a) in the international system over which states do not exercise the normal prerogatives of sovereignty, and b) to which norms provide for universal access for economic, political, scientific, cultural, and sometimes military purposes, for those states with the requisite technological capabilities. *Aaron L. Connelly, B.A.* 8

This is readily observed in each of the domains in which the commons has been said to exist and is one of the most accurate descriptions of the Commons. Without the law of the sea, which restricts the writ of sovereignty to increasing degrees as one travels further from shore, there would be no maritime commons. Without the Outer Space Treaty, which declares that outer space is “not subject to national jurisdiction,” most low earth orbits would involve violations of state sovereignty, and there would be no space commons. Without the web of
bilateral treaties and international cooperation providing for access to each other’s national airspace, there would be no air commons. 9

In both the maritime and space commons, states have explicitly given up the prerogatives of sovereignty through international agreement. In the air commons, they have reserved these prerogatives, but have concluded a web of bilateral treaties and international agreements that facilitate the precedence of norms of a commons over the prerogatives of sovereignty. In each case, these regimes also provide for universal access, given possession of the requisite technological capabilities even for landlocked countries.10

To bring up the strategic significance of the commons, it is important to explore how they play a role in the global economic framework. The value of world trade as per 2014 figures is about USD 18 trillion. About 70 per cent of world trade by value and 80 per cent by volume are carried by sea. Only a miniscule percent is by air and there is substantial trade, by land, particularly Europe, North America and Eurasian regions. About one per cent of the volume and 20 per cent of the value is by air. Air Carriage of freight is mostly of high value, electronic goods, including the latest smart phones, computer chips, perishable goods, medical supplies, vaccines, organs etc. The remaining is accounted for by land transport and rail.11

To bring these figures into perspective vis a vis cyber space, it is estimated that daily transactions on SWIFT (Society for Worldwide Interbank Financial Telecommunications) is about USD 10 trillion.12 The global critical infrastructures are composed of both public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information technologies and telecommunications, energy, transportation, banking and finance, chemicals including hazardous materials, and postal
services and shipping. Cyberspace can now be described as their nervous system—the control system of the Modern world.  

It is now evident as to why Cyberspace has been described as the strategic high ground of the 21\textsuperscript{st} century the domination of which is the prize pursued by global powers. This explains the reasons for the 2016 US budget for cyber security\textsuperscript{23} being larger than their nuclear weapons budget and the Chinese declaring their intentions to concentrate on cyberspace and information warfare.

**Cyber Commons**

![Vice Admiral Arthur Cebrowski](image)

Vice Admiral Arthur Cebrowski

The first to describe the existence of a commons in cyberspace was Vice Admiral Arthur Cebrowski (Retd) in 2004, while he headed the Pentagon’s Office of Force Transformation. Though Cebrowski did not seek to define the global commons, he did seek to describe it. Cebrowski compares the cyberspace commons to the maritime commons of the 19\textsuperscript{th} and 20\textsuperscript{th} century, suggesting that cyberspace will be the most important strategic commons of the 21\textsuperscript{st} century, just as the maritime commons had been the most important strategic venue in the preceding centuries. He notes the importance of the cyberspace commons to trade and communication. But he suggests that the cyberspace commons will differ in four important ways from the maritime, air, and space commons: the entry fee is much lower, and thus access is influenced by non-state actors more
than states; it is non-dimensional; it is expanding at a non-linear rate; and “its characteristic interactions more closely approximate the human condition, making it an enormously complex operating domain.” Despite Cebrowski’s untimely death in early 2005, the “cyberspace commons” language was included by the Defense Department in its 2005 National Defense Strategy.14

Cyberspace can be broadly divided into a physical layer and an information layer. Each layer operates under a different set of dynamics. It is easily understood that the information layer’s existence is dependent upon the continued existence of the physical layer. Less easily understood is that this is not a one-for-one dependency. Parts of the physical layer can be destroyed, damaged, turned off or replaced without effecting the destruction of proportional value in the informational layer. This is, in part, because of the increasingly common information assurance practices, which create redundancies within the information layer.15

Second, cyberspace’s information layer is a social construct. Much of the value in cyberspace is stored not only in the code on servers, but also in the various patterns of interaction that take place via the exchange of code between servers. For example, the value of an enterprise like Facebook is not only primarily in the data stored on its servers, but in the way that Facebook facilitates interaction that result from the connection of people around the world. The international community is slowly realising the intelligence potential and economic value of this record of interactions. It is thus the most efficient domain for the transmission of ideas, goods, and capital. If the physical layer of cyberspace is destroyed, damaged, or turned off, these networks on the information layer persist in the minds of those who build and use them. If they are of value, participants are likely to seek to reestablish them either using other elements of the physical layer, or by building new physical infrastructure to support them.16
Third, cyberspace is a human-made domain, subject to quick and constant reorganization and reconstruction. This is true of both the physical layer, which is comprised of terminal appliances, fiber-optic cables and radio frequency spectrum, as well of the information layer. 17

Fourth, cyberspace is a venue for military activity. This includes a spectrum of activities across the political, strategic, and tactical levels—from the formation of alliances, to competition for superiority, to low-intensity conflict, espionage and surveillance to complete warfare. Scholars of cyber war describe a range of military activities in cyberspace, from surveillance to coordinated Dedicated Denial of Service (DDoS) attacks. Scholars of security studies have also reached a consensus that cyberspace constitutes a separate “domain” of warfare, alongside the maritime, land, air, and space domains. This elevation of cyberspace to domain status has gradually occurred over the last ten years. 18

Fifth, barriers to entry are low. One no longer even needs a personal computer and landline connection to take advantage of the benefits that cyberspace provides, given the ubiquitous smart phones and wireless connectivity in both the developed and developing world. But barriers are not only low for individuals; they are also low for those interested in using the Internet for military activities. Building a navy, air force, or fleet of satellites and space weapons are all extremely capital intensive and costly endeavors. In this sense, the cyberspace domain is similar to the land domain, where barriers to entry are also very low. 19

The Fallacy of the Cyber Commons

Though governments have asserted sovereign control over the Internet in response to perceived threats, the authority to
govern the Internet has always resided with the state, specifically with the U.S. government. The Internet is a DARPA invention and at the most basic level; the United States Government controls the current system of organization of the Internet. The United States Commerce Department holds ultimate authority over the disposition of the official root zone file—simply defined as the file, which directs the Internet Protocol (IP) address of every end user. This is the technological hierarchy that directs all traffic on the Internet. The U.S. government has strategically taken a hands-off approach to this responsibility, contracting it out to either academic or non-profit institutions; all attempts for multinational control have been stonewalled. But this arrangement may not be sustainable especially after the Snowden revelations.  

In recent years other governments have challenged American control of the official root zone file. Governments around the world are increasingly unhappy with the custodianship of the Internet Corporation for Assigned Names and Numbers (ICANN), the Los Angeles-based non-profit contracted to administer the file since 1998. As this article is written there was an announcement that the US control of the Internet has ended. The announcement; to end direct US government oversight control of administering the Internet and commit permanently to a slightly mysterious model of global “multi-stakeholderism”; whatever that means. This falls far short of attempts by other nations to have the United Nations, International Telecommunication Union to take over its job.  

Much of the assumption of the existence of a cyberspace commons appears to follow from a basic recognition of cyberspace’s network-like qualities under different national jurisdictions but once we understand that the key networking hardware, protocols and big data companies in numerous spheres are all American, in combination with the recognition that cyberspace constitutes its own domain of warfare,
alongside the land, maritime, air, and space domains. 22 Given this assertion of state sovereignty over cyberspace, and the lack of any norms of universal access, it is evident there is no commons in cyberspace. The construct of a commons in cyberspace appears to be a careful orchestration of US strategy to promote their interests and to consolidate their grip on this vital domain through a strategy of promotion of big US-centric MNC’s.

As we peer into the future, it is evident that the USA, the dominant global power, would like to preserve the chimera of a Cyber Commons that it can continue to dominate, the contours and dimensions of which are yet to emerge. A future Cyber Commons if it ever evolves should be a physical layer of access based on open source technologies controlled by the UN. Such a physical layer could be based on non-terrestrial platforms (preferably space based) to prevent nation states from exerting sovereign control. The information layer eventually will evolve wherein data generated in a sovereign jurisdiction would be stored within its territorial jurisdiction. Not doing so would result in big data companies like Google and Facebook having tremendous ability to influence economic, diplomatic, military and political activities in other nations. The realities of today are that control of the physical layer rests with the Original Equipment Manufacturers (OEM’s) and not with the system/network administrators who have an illusion of control by their perceived ability to configure the Graphical User Interface of their appliances. The vast majority of the information layer is also firmly in the grip of the Big Data companies, which are primarily of US origin and have their server farms located in USA.
China and Russia

When you look at the cyberspace domain outside the west, it is but natural to examine the state of affairs of the two open strategic challengers of the west, China and Russia.

China with a 700 million plus population online is the largest market in cyberspace. Although it has embraced the Internet along with the rest of the world, China has always enforced a strict control on the content of the net, which was called the ‘Great Firewall of China’. Western literature was widely critical of these controls and effectively tied them to the idea of an authoritarian political system suppressing free speech to cling onto power. The West was also widely critical of state supported hacking by Chinese groups and the world was widely outraged by the specter of massive espionage; stealing of intellectual property of top Western companies, dissident groups, neighbouring countries, international bodies etc. These reports were mostly true and still continue, but dramatically lost steam after the Snowden revelations and the perfidy of the US and the NSA with most of the silicon valley technological firms exposed as being part of a global surveillance infrastructure. The US has since tried to differentiate between the economic espionage by the Chinese, and US surveillance chiefly being supportive of the global war on terrorism with little success.

The Chinese by its policies have successfully midwifed such companys as e-commerce giant Alibaba Group Holding Ltd., online conglomerate Tencent Holdings Ltd. and information aggregator Sina Corp, which enable Chinese citizens to enjoy most services Westerners use, without needing Google or Facebook. The Chinese government is directing financial and policy support toward domestic firms that are developing
semiconductors and servers that can replace ones provided by Western firms. China has also unveiled Internet Plus, a strategy to incubate Chinese companies that integrate mobile, cloud and other types of computing with manufacturing and business. Many Western companies have started conforming to Beijing’s rules to take advantage of the Chinese markets. LinkedIn structured its Chinese operation as a domestic company and agreed to comply with Chinese rules. Hewlett-Packard, sold a majority stake in its China server, storage and technology services operations to a Chinese company after it came under pressure in China following revelations that U.S. officials collected information abroad using infrastructure produced by American companies. 23

China is seeking international validation for its efforts. Earlier this year, China led Russia and some Central Asian countries in proposing the United Nations adopt an Internet “code of conduct” that would effectively give every government a veto over technical protocols interlinking the global Internet. As social media helped topple regimes in the Middle East and northern Africa, the People’s Liberation Army publicly warned that an Internet dominated by the U.S. threatened to overthrow China’s Communist Party. The Chinese declared that the Internet represented a new form of global control, and the U.S. was a “shadow” present during some of those popular uprisings. On July 1 2015, China’s legislature passed a new security law asserting the nation’s sovereignty extends into cyberspace and calling for network technology to be “controllable.” A week later, China released a draft law to tighten controls over the domestic Internet, including codifying the power to cut access during public-security emergencies. Other draft laws under consideration would encourage Chinese companies to find local replacements for technology equipment purchased abroad and force foreign vendors to give local authorities encryption keys that would let them control the equipment. 24
Cyberspace in Russia was largely considered a zone of relatively free expression and little state involvement. Following the rallies of the Russian opposition in 2011-2012 and the onset of the Arab Spring in both of which the Internet played a significant role, cyberspace and its potential for political disruption was taken note off. The Snowden revelations added to Russian threat perception and military actions in both Ukraine and Syria and the resultant tensions with the west prompted a series of legislative, technological and diplomatic measures aimed at preventing domination of cyber space by the west. 01 Sep 2015 saw the enactment of Russia’s new law on personal data, which requires foreign companies that handle personal data of Russian citizens to process and store such information inside Russia. To comply with the law, many have already moved servers inside the country’s borders. EBay, Google, and others are in the process or have already moved user data in country. EBay is transferring data from Switzerland to Russia. Google has moved some servers’ in country to comply with data localization laws and announced plans to discontinue development work in Russia and move its engineering operations there to other countries. Adobe said it would close its offices in Russia, and Microsoft closed a developer office in the country, moving a significant portion of the operation to Prague. 25

Russia has banned use of foreign software for many categories of government services and the new changes will include the introduction of ten percent levy on software sales in Russia, the abolishment of VAT preferences for software developers and the design of Russian analogues of imported software. It is planned that the revised doctrine will also encourage the establishment of software production within Russia and increase the powers of law enforcement agencies to block banned information spreading through anonymous networks.
This currently occurs in accordance with court decisions and as part of extrajudicial procedure. 26

Russia has reportedly run tests to see if it can remove itself from the World Wide Web to stem the flow of information to and from foreign countries. The tests were run to prepare for an information blackout in case of a potential domestic political crisis. The goal was to see if Russia’s Internet could continue to function even though it was cut off from the global Internet. The Putin regime has publicly stated that the freedom of the Internet will be protected but the state will take measures to defend itself. 27

**Indian Calculus**

USA, the world leader in innovations in Cyberspace, and the original proponent of concepts of Information Warfare, today controls most of the Information repositories of the world through their giant MNC’s and has been successful in influencing the thought processes of the majority of the global population where free flow of data has been linked to freedom of expression and ideas. Such a construct has been propagated with the connivance of their Western allies.

The hollowness of these ideas were exposed by the Snowden revelations and recognized recently by the European Union in a landmark judgment where the principle of ‘safe harbor’ 28 used to transfer data across national boundaries was stuck down. This has profound implications for the world wherein clear delineation has been made between freedom of speech, ideas and personal data.

In the Information Age, although traditional methods of power projection is still relevant, the advantage will always belong to nations that can effectively garner and process the huge information flows of Cyberspace to give a competitive
advantage to their nation in all spheres; be it military, diplomacy, trade etc. The global ICT market is poised to undergo a revolution post Snowden. The initial ripples can already be seen in the recently concluded BRICS conference where Brazil, Russia and South Africa urged India to take the lead in building a new global ICT architecture based on Open Source Technologies.

India has still not exploited this situation fully, although the political leadership has made the right beginning with the *Make in India* initiative. A very effective and entrenched software industry catering to the West and their representative industry bodies in collusion with sections of the bureaucracy in both the military as well as the civilian sector has opposed transition to indigenous and open source technologies with out fully understanding the strategic dimensions of the issue. Such a change can, not only kick start domestic manufacturing and entrepreneurship but will find huge markets overseas. This strategy will also find increasing backers from nations who want a multipolar world and are in consonance with India’s stated strategic aims.

**Conclusion**

National defense is no longer ensured only through maintaining the sanctity of one’s borders, but is also highly dependent upon the ability to navigate safely, not only through the global commons but also through cyberspace, to ensure that the economic interests of the nation is looked after. These commons—sea, air and space plus Cyber Space are at present dominated by the USA who does that by leveraging two pillars of power - the USD as reserve currency and American military power funded by fiat dollars. The American dominated world order has permitted other nations including China to economically progress as long as they do not upset the current world order.
American strategic thought process identifies Russia, China and India as long term strategic rivals, India less so than Russia and China. Although American strategy currently involves shoring up India as a counter to China it is uneasy on the long term implications of Indian power potential and views India as potentially a long term rival that can challenge American domination. To that extant the Indian nation, if it has to reach its full potential will have to make an independent cyber strategy based on indigenous technologies as otherwise it can be open to strategic disruption from the cyber medium as the diverse population mix is more susceptible to internal schisms in comparison to a much more uniform Han Chinese and Russian population to a Hybrid threat matrix. The short term threat to India might be from Pakistan and China, but these threats are not existential in nature unless there is a nuclear war. As the Indian economy grows the West might increasingly tend to keep India disbalanced to have leverage, as Western strategy tends to look at capabilities than intentions. The Indian nation by its very size is a long term strategic competitor for China as well as the USA for global leadership and the threats to it from realising its just place in the comity of nations in a globalised and nuclear environment are more likely through internal disturbances exploiting the numerous social, regional, religious, economic and political faultlines intelligently orchestrated using cyberspace. The ocean of Cyberspace, the strategic high ground of the 21st century, is without doubt firmly in the grip of the USA with only China even attempting to challenge it. A nation the size of India, with its latent power potential and huge diversity of population cannot afford to ignore these realities. The need of the hour is understanding of strategic realities and a well-nuanced plan of action.
Bibliography


Secretariat: B-55, Birsa Munda Rajpath Harmu Housing Colony, Ranchi Jharkhand Pin - 834002 India Ph.: +91.651.645 8865

Delhi: K-51 (First Floor) Green park Main, New Delhi - 110016

email: secretariat@cyberpeace.net

www.cyberpeace.org