# Cyber Warfare and Global Power Politics

Afeera Firdous*

## Abstract

Every technological advancement brings more power to the countries acquiring these capabilities and a new set of threats as well. Along with that, the struggle for power among states also begins. The development of computer and information technology is not an exception to this phenomenon. New threats to personal and national interests emerge as states acquire and develop this new technology. This paper analyzes power asymmetry in major states developing non-contact and stand-off capabilities in warfare such as in the cyber domain. It also examines the international discussion on cyber governance and cyber arms control, cyber-related policy documents and military units, and state-sponsored cyber-attacks. In the end, the paper describes the regional context of cyber geopolitics i.e. how both, India and Pakistan, are evolving their respective capabilities in the cyber domain.

## Keywords

cyber warfare, cyber geopolitics, Information Technology, cyber governance.

## Introduction

Every technological advancement enhances the power potential of a country developing or acquiring it. This also inevitably triggers an arms race. The development of computer and information technology is not an exception to this rule. The threats to personal and national

* Afeera Firdous is Research Assistant at Center for International Strategic Studies (CISS), based in Islamabad.

interests are being identified by the states as the new technology is developing. Many countries have assessed these threats to be so significant that they have designated cyber and information domain as the fifth operational domain[1] after land, sea, air and space. The power struggle (in cyberspace) between major states has already started dominating the virtual/cyber world and to gain maximum control.

Cyberspace, however, is still an evolving domain of human interactions, with its peculiar security and defense concerns for the states. Internet based information and communications systems have become deeply rooted in a country's political, economic, and social networks. Though individuals and civil society members, these days, have emerged as important players in national and global politics, but states still retain the ability to do surprising and frightening things that no collection of netizens can carry out. Countries use their cyber powers to attack, espionage, influence, trade and steal from each other. According to Cyber Operations Tracker,[2] twenty eight countries were found to have been involved in more than two-hundred and fifty cyber-attacks on other states from 2005 to 2018.[3]

This article examines whether the power politics in cyberspace can reshape the world order from a unipolar to a bipolar or a multipolar world, or it will remain unaffected by cyber domain operations. This paper would also analyze how such activities may effect a crisis situation between two adversaries. Furthermore, it evaluates military capabilities of the US and China in cyber domain which include official cyber-related policy documents, cyber units, cyber commands, and cyber-attacks on each other.

This research is organized into three sections. In first section 'governance of cyberspace', and the current status of cyber governance by the US, China and Russia is discussed. This section also includes debate on international rules and regulations for cyber governance and cyber arms control. Next part of this paper examines cyber and targeting capabilities in military domain in terms of emergence of cyber commands, release of official cyber policy

documents, and state-sponsored cyber-attacks including online surveillance and espionage operations. Finally, this paper analyses cyber geopolitics in South Asia; how India and Pakistan are enhancing their respective capabilities in cyber domain.

## Governance of Cyberspace

As a medium, cyberspace has different dynamics compared to other operational domains; i.e. land, air, and sea. Unlike these three domains, cyberspace has no physical boundaries. It can be accessed from any part of the globe which brings with it issues related to cyberspace governance. There are two major issues which need to be addressed by nation states with regards to cyberspace governance: domestic laws and international regulations.

After Russian cyber-attacks on Estonia[4] in 2007, cybersecurity is considered as a global challenge and a tier-one security threat to sovereign nations. Many countries, for years, have been trying to have a rule-based cyberspace governance systems. However different states have diverse views on how the cyberspace should be governed. The answer to this query sometimes comes as having open internet, governed by multi-stakeholder and at other time showing preference for cyber sovereignty.

Some western experts have emphasized the concept of cyber sovereignty and spirit of internet, which rests on the notion of unrestricted interconnectivity. Both these concepts, however, are considered contrary to each other.[5] In case countries agree on cyber sovereignty, it may lead to creation of separate cyberspace by every state, resulting in dismantling the very concept of internet. The idea of cyber sovereignty also agitates against the issues of human rights, freedom of speech, and free flow of information. Compared to that, the notion of free internet and current pattern of multi-stakeholder governance of cyberspace poses threat to some countries as it provides freedom to countries to intervene into the internal matters

of other states. Multi-stakeholder governance (of cyberspace) model can also become an instrument of bias against a particular set of countries, serving hidden purposes for other states. Another difficulty of cyberspace governance is how and in whom the administrative authority in cyberspace be vested.[6]

## Asymmetry in Cyberspace

As the internet came in public sphere in the 1990s, cyberspace has grown at a fast pace which created asymmetry, of resources and capabilities, among states. Rather than achieving progress in development of network technologies, developing countries are further marginalized due to lack of resource and capabilities in cyberspace field. Moreover, this marginalization of developing countries may increasingly weaken their geopolitical position globally. Developed countries, on the other hand, with significant developments in industries and technologies (especially in cyberspace and information technologies), research and development, and innovation can further expand their global influence and power.

There are some aspects[7] which reflect the asymmetry of resources and capabilities among countries such as number of internet users in different regions (internet users' geographical distribution); wide gap in infrastructure and facilities related to information technology, data and networks in developed and developing countries; and advantage of developed countries in management of resources and facilities to establish and secure their own physical infrastructure of cyberspace operations around the world.

## US-China Rivalry

In world politics, not many issues, between the US and China, have escalated instantly and caused so much friction and conflict, as cybersecurity.[8] Both countries have recognized cyberspace as crucial to their economic and national security, and have formulated several domestic strategies and doctrines to shape the Internet and its usage.

Currently, both the US and China perceive the other as a significant, if not the major, obstacle to pursue their interests in the cyber domain. There are many issues on which the US and China disagree rigorously including international governance of cyber domain, the definition and concepts in cyberspace, legitimacy of online surveillance and espionage, and the balance between the values of national sovereignty and free flow of information.

In the business domain, tech companies from the US and China contest over expanding their customer base, global standards, and their access to markets. However, both countries have common interests in some critical areas too, such as protection from third-party attacks on their critical infrastructure and developing confidence-building measures (CBMs) in the field of cyber conflict.[9]

Moreover, the competition between the US and China is also continuing and they are quickly slipping into a dispute in and over the cyber domain. The conflict in cyberspace between the two technological giants will lead to serious risks and difficulties for both countries in terms of their economic and technological interdependence. If continued unabated, it may lead to serious repercussions internationally on industrial and technological basis, as well as in terms of their commercial utility, and defense and security applications.

Different factors are pushing both the US and China on a confrontational path. Some of which arise from the decline in their overall mutual relationship, particularly in the trade realm, and others are caused by the growing tensions induced by Chinese moves to expand its influence in neighboring regions in Asia. But cyber dynamics have intensified the tensions. Notably, the intense competition is becoming apparent in their technological achievements as China's cyber intrepidity progressively catches up with that of the US. It is far easier to point out the drivers of deterioration in bilateral relations between the two biggest economic powers in terms of

politics, economics, and security than to rectify them. Some of the steps taken by both countries in these domains are not only counter-productive and destabilizing, but sometimes outright escalatory. This is a classic case of security dilemma among two countries, where each feels threatened by other's actions, take steps to ensure their security but practically, both states are left worse off.

Both countries suspect each other of using their critical information technology infrastructures (especially companies) such as IBM, Oracle, Cisco, and now Huawei's 5G technology against the other side. China and the US see the internet's inherent potential to spread rumors and false information generating suspicion. This feature of the internet could be used to cause unrest in a society and threaten a country's social and political cohesion. Moreover, China dreads that Western countries may use such practices to project and propagate their ideology and values of openness and free speech which it believes would be politically destabilizing. Chinese also suspect that Twitter and other social platforms were used during Iran's 2009 election fraud[10] protests.

## 5G and US-China Competition

5G or the fifth generation of mobile technologies, is increasingly being identified as the ideal source for spurring a revolution in mobile and cellular data. Many aspects of the industry, including urban management, remote healthcare, precision agriculture, and digitized logistics, would profit from 5G as a technological stimulus of its kind would not only increase productivity but also drastically enhance the efficiency. It is estimated that by the year 2035, 5G would have raised global economic output by $13.2 trillion in goods and services.[11] Moreover, 5G will drive towards the creation of 22.3 million jobs in the shape of a 5G value chain, i.e. the operators, original equipment manufacturers, consumers, and app developers.[12]

That's why, technologically advanced countries such as the US, China, and South Korea have the incentive to invest in 5G capability and

establish 5G networks and hubs across their respective territories to instill an economic stimulus. Recently, the United Kingdom also joined the list of countries interested in establishing an array of 5G networks with the partnership of Huawei which instigated a new conflict between the US and China. The US and Trump administration voiced their concerns on the British decision to collaborate with the Chinese company, alleging that China is involved in illegal trading practice and intellectual property theft,[13] and this is nothing more than China's attempt of attracting states with economic incentives to integrate them into its foreign policy initiatives.

The US views Huawei as a front for China to carry out espionage and gain access to sensitive information and credentials. This is especially true when it comes to the US perspective of growing Huawei influence in the global 5G supply chain. US intelligence circles are concerned that by allowing Huawei to penetrate the communications network, it could gain complete access to it and even shut it down if a cyber-war were to ensue. The US also believes that Huawei would be bound to share information with the Chinese government if a request was ever made by the Chinese authorities for the sharing of data and information. If the US allows UK to cooperate with Huawei, the 'Five Eyes" intelligence-sharing alliance (between the US, UK, Canada, Australia, and New Zealand) would be jeopardized.[14]

Apart from security concerns, there are distressing economic concerns on which Trump administration officials have gone so far to call Huawei a 'Mafia' which uses unethical and illegal market practices in market competition.[15] The US is apprehensive that in light of the UK's choice to side with Huawei, the UK may now be moving away from the sphere of the US influence and that might encourage other major European powers to follow suit. The issues of 5G and dominance of different countries in this technology will persist for longer period of time due to its impact on economic and security facets of a state. 5G technology will play important role in states'

assertions / dominance in technological, security and economic domain.

## International Discussion on Cyber Arms

After the first Information Warfare Doctrine[16] was released by the US, in 1998, Russia brought the discussion on 'Information and Communication Technology (ICT) terming it as a threat to peace and stability' to First Committee of the UN General Assembly (on disarmament and international security).[17] This discussion ultimately resulted in creation of a group of governmental experts (GGE) on developments in the field of ICT in the context of international security. The first meeting of GGE on ICT evolution and international security was held in 2004.[18] GGE (on developments in field of ICT in the context of international security) met five times during the period 2004-17 (**Table 1**).

During the GGE discussions, Russia suggested to contain the actors (states) having greater cyber capabilities restrain the flow of information to the limits of national boundaries. Russia and China also advocated a 'multilateral regulatory process' to address the use of ICT for military purposes. On the other hand, the US framed its whole argument around the action of state-sponsored activities targeting against other states, rather than discussing domestic information security threats.

On the recommendation of 2016-17 GGE, an open-ended working group (OEWG) was established to build norms on earlier work of five meetings of GGE and introduce changes, if necessary. The US vigorously opposed the creation of OEWG and proposed a separate UNGA resolution on responsible state behavior in cyberspace.[19] However in December 2018, the UNGA issued the roadmap for the period of 2019-2021 (Tentative Timeline Fig-1[20]) in which both processes, GGE and OEWG, have to discuss the issues of security in the use of ICT.[21]

**Table 1**. GGE on Developments in the Field of ICT in the Context of International Security, 2004-17[22]

| Years | No. of members | Chair | Participating States |
|---|---|---|---|
| 2004-5 | 15 | Russia | Belarus, Brazil, China, France, Germany, India, Jordan, South Korea, Malaysia, Mali, Mexico, South Africa, UK, US |
| 2009-10 | 15 | Russia | Belarus, Brazil, China, Estonia, France, Germany, India, Israel, Italy, South Korea, Qatar, South Africa, UK, US |
| 2012-13 | 15 | Australia | Argentina, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK, US |
| 2014-15 | 20 | Brazil | Belarus, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, South Korea, Malaysia, Mexico, Pakistan, Russia, Spain, UK, US |
| 2016-17 | 25 | Germany | Australia, Botswana, Brazil, Canada, China, Cuba, Egypt, Estonia, Finland, France, India, Indonesia, Japan, Kazakhstan, Kenya, South Korea, Mexico, Netherlands, Russia, Senegal, Serbia, Switzerland, UK, US |

While assessing two approaches, it is clear that Russian-sponsored OEWG aims at controlling the cyber arms with legally binding norms, whereas the US proposed resolution is focused on voluntary and non-binding measures. GGE discussions were inconclusive as the US and Russia/China had widely divergent stands on basic issues such as intentions, concepts and definitions.

During GGE process, sufficiency and adequacy of the existing international law to guide state's behavior in cyberspace came into discussion. In dialogue on international law, China and Russia usually advocate a rule-based approach, while the Western countries takes policy-based positions. The former approach, according to an expert, regards the law as normatively strong but restricted in scope; the latter sees the law as normatively weak but wide in scope.[23] While

assessing the discussion on governing cyberspace, it is evident that states reflect, their behavior or way of governance, in real politics into cyber domain as well.

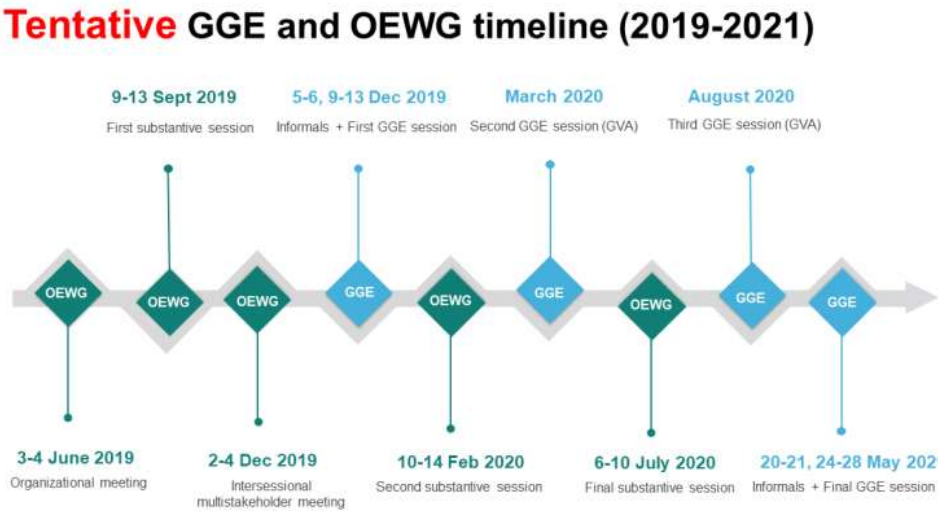


*Figure 1 Tentative timeline of the GGE and OEWG (2019-2021)*

**Military Competition in Cyberspace**

As the countries recognized cyber domain as an operational realm, the realization of the need to incorporate cyber defense/offense edifice into their existing military structures started to emerge. Till the second decade of the twenty-first century, many countries started focusing on developing cyber policies and strategies, the establishment of cyber mission force, cyber units, and, later, cyber commands, and cyber-attacks to coerce or punish the adversary. Hence, the world may be witnessing the evolution of a new field of strategic competition and military dominance.

Although the 'strategic thought on warfare in cyber domain' is yet in its infancy, a few nations have already established cyber commands component in their armed forces. These include the US and North

Atlantic Treaty Organization (NATO), China, Russia, Britain, Germany, France, Israel, and India. On the other hand, some countries are in the process of incorporating these components into their armed forces. In fact, during the last two decades, cyber domain has been used to initiate operations such as espionage, sabotage, and subversion against their opponents.[24] Major examples in this context are reportedly Chinese cyber-attacks on several secure systems of the US government offices such as the Department of Defense (DoD), Department of State, Department of Homeland Security (DHS), National Aeronautics and Space Administration (NASA), and the Office of Foreign Commonwealth in the UK,[25] 2007 cyber-attacks on Estonia and 2008 computer network operations on Georgia,[26] and more significant and coordinated cyber operation on Iran's nuclear facility, Stuxnet.[27]

## Policy Documents

In the beginning, the US and China were inspired by different motivations for the development and expansion of cyber capabilities. China commenced developing capabilities for cyber combat in response to the shifts in its competitive environment. The first policy document which initiated this development is the second version of Military Strategic Guidelines revised by the former President Jiang Zemin.[28]

The Military Strategic Guidelines (MSGs) were drafted by the Central Military Commission in 1949, to respond to consistent and critical developments in some areas of assessment such as international order, regional security environment, domestic situation, and nature of warfare itself.[29] The document was subsequently revised and updated to deal with changing threat perceptions of Chinese legitimate position in the world order. MSGs determined the course for the People's Liberation Army's (PLA) strategic transformation until mid-century and continued a set of indicators and goal. The first

indicator was to form a strong base for the 'informationization and mechanization' for Chinese armed forces by 2010. The next indicator is to fully automate the force and achieve the primary stages of informationization by 2020. The last indicator is to gain information dominance by the PLA by 2050.[30]

Since it is impracticable for China to develop the conventional military power comparable to the US in a short time-frame, China has concentrated its efforts on developing its ability to manipulate the key vulnerabilities of the US such as its high dependency on the Internet and its inadequate abilities for cyber defense.[31] China's Military Strategic Guidelines remained as the central policy document which gave the strategic guidance to China to modernize and prepare the PLA for the wars in twenty-first century. There are conflicting government accounts about the dates of MSGs' revision. An expert on Chinese military, David Finkelstein, however insists that the document was last modified in 1993 and the succeeding accounts of the document i.e. Military Strategic Guidelines for the New Period still follow the original core goals of the PLA.[32]

Unlike the Chinese objectives, the US initially developed and advanced military capabilities in the cyber domain to overcome the vulnerabilities of its critical national infrastructure, especially in telecommunications, energy, banking and finance, transportation, water systems, and emergency services.[33] The US issued its first policy document, Presidential Decision Directive-63 (PDD-63), drafted by the National Security Council of President Clinton in 1998. PDD-63 mandated the US government to draw some policies to overcome vulnerabilities in its national critical infrastructure against the growing threat.[34] In February 2003, the US government presented a cybersecurity strategy, for the first time, which was later revised and extended as a national cybersecurity policy in December 2003. The National Strategy to Secure Cyberspace designed a comprehensive plan to ensure the security of critical infrastructure systems, and

mandated the government to prepare plans to fight potential conflicts in the cyber domain.[35]

In addition to this, a national cybersecurity policy, for the federal government and relevant agencies, was established by the development of Homeland Security Presidential Directive-7 (HSPD-7). The purpose of this directive was to analyze and prioritize essential resources and critical infrastructure and defend them from terrorist attacks in cyberspace.[36] Department of Defence (DoD) also issued its cyber strategy in July 2011.[37] Later in September 2018, the White House presented a national cyber strategy comprising four key points: first, to protect the people, homeland, and way of life by defending networks systems, functions and data; second, to promote prosperity by sustaining a secure and growing digital economy and promoting national innovation; third, to preserve peace and security to dissuade and punish those who employ cyber domain maliciously; and fourth, to advance the influence to spread the key principles of an open, interoperable, strong, and secure internet.[38] In 2018, DoD also revised its cyber strategy. Revised policy aimed at following five objectives; first, to establish a more lethal force; second, to have the ability to contest and deter others in the cyber domain; third, to strengthen partnerships and engage with new allies; fourth, to reform the department; and fifth, to bring in new talent.[39]

## Cyber Military Units/Commands

With different strategic utilization of the cyber domain concepts, China and the US formulated cyber military units to carry out computer network operations (CNO) accordingly. In China's case, much data on PLA's cyber units and command as well as the operational control of employing CNO is with the PLA's Third and Fourth Departments of the General Staff Department.[40] The Third Department was established during the 1980s and the Fourth Department during the early 1990s.[41] PLA's Third Department, which

is China's central signals intelligence organization, is bound to carry two tasks; computer network defense (CND) and computer network exploitation (CNE). While, The PLA's Fourth Department is the electronic countermeasures organization which is responsible for computer network attacks (CNA).[42]

The US started establishing a coordinated military response to possible cyber-attacks in 1998. A Joint Task Force on Computer Network Defense (JTF-CND) was formed under PDD-63. JTF-CND was tasked to protect the computer networks and systems of the DoD.[43] Though JTF-CND was not designated as an independent cyber command, but it served the defense establishment at the strategic level through the National Infrastructure Protection Center[44] (NIPC).[45]

In December 2003, the DoD started to focus on offensive missions alongside with defensive operations in cyber domain. As the JTF-CNO was not able to perform both, offensive and defensive, operations effectively, offensive operations were first assigned to the National Security Agency (NSA) under the US Strategic Command but in 2004, a new component, named Joint Functional Component Command – Network Warfare (JFCC-NW), was created under the US Strategic Command to carry out offensive operations.[46] The US Cyber Command (USCYBERCOM), established in 2009, has a stated objective: "to direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[47]

Each of the military service provides support to USCYBERCOM such as Army Cyber Command (2nd Army ARCY), Air Force Cyber Command (24th Air Force AFCY), Navy Fleet Cyber Command (10th Fleet FLTCY), and Marine Corps Forces Cyberspace Command (MAR4CY). DOD began to build a National Cyber Mission Force (NCMF) in 2012 to carry out DoD's cyber missions. The NCMF consists of 133 teams that are organized to meet DoD's three cyber missions. Specifically,

National Cyber Mission Force teams support these mission sets through their respective assignments: Cyber National Mission Teams, Cyber Combat Mission Teams, Cyber Protection Teams, and Cyber Support Team.[48] NCMF teams reached full operational capacity at over 6,200 individuals in May 2018. In structural terms, the National Cyber Mission Force is part of the United States Cyber Command.

The DoD also revised the mandate of its Defence Communications Agency, which later became the Defence Information Systems Agency (DISA). The mission of DISA is to provide and ensure command and control, and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfare across the full spectrum of military operations.

**Cyber-attacks**

Increased intensity and scope of cyber-attacks are another significant indicator of the competition for military superiority in cyberspace. More sophisticated and extensive cyber attacks were discovered as the competition in cyberspace escalated between China and the US (and its allies). Available data indicates that China conducted six major cyber-attacks against the US from 2003 to 2012.[49] On the other hand, China's internet is also one of the most frequently attacked. According to a report issued by the Beijing Knownsec Information Technology in February 2019, the country experienced the highest number of distributed denial of service attacks (DDOS) in the world in 2018; approximately 800 million a day.[50]

A strategic and ongoing series of CNE attacks started in mid-2006, codenamed Operation Shady Rat, believed to be purported by Chinese hackers. These attacks affected forty-nine companies and government agencies in the US, including defense contractors such as Lockheed Martin, Northrop Grumman, and BAE Systems.[51] The attacks were considered critical because these contractors had a central role in the

production of the F-35 Joint Strike Fighter in addition to other highly classified US military weapons.[52]

As the Stuxnet attack, collaborated by the US and Israel against Iran, became the first recognized example of state-sponsored cyber-attack which described the potential efficacy of cyber capabilities of a state.

**Regional Context**

In the South Asian context, both India and Pakistan have realized the significance of the cyber domain and its related vulnerabilities in different ways. In a way, both countries acknowledge the threat of criminal activities and scams, terrorism, and state-sponsored activities on cyberspace; but in Pakistan's case, the response to such activities is slow or not publically known. Nevertheless, in an increasingly intense environment between India and Pakistan, after Prime Minister Modi's election, both countries are active in cyberspace to exploit vulnerabilities of each other.

Among the South Asian countries, India has been more prominent in participation in international and regional discussions on cyber norms. India participated in four out of five GGE meetings, on Developments in the field of ICT in the context of International Security, organized by the UN General Assembly (see Table-1), since 2004. On the other hand, Pakistan only attended one out of five of these meetings.[53] In 2017, India hosted and chaired the 5th Global Conference on Cyberspace (GCCS), initiated by the London Group in 2011.[54] The event was attended by representatives of government, private sector and civil society, to encourage cooperation in cyberspace, discuss global cyber norms for responsible behavior, and increase cyber capacity building.[55]

In August 2019, India also hosted and organized the 'Cyber Workshop' for Shanghai Cooperation Organization (SCO) member states,[56] but Pakistan opted not to participate in the workshop. In recent years, Pakistan also organized some conferences; these include; Build Asia 2019 International Exhibition & Conference[57] and International

Conference on Frontiers of Information Technology - FIT,[58] but most of the events addressed the technical issues related to IT. Pakistan's government institutions have focused on cyber-crimes and pay lesser attention to policy issues such as cyber-security policy and strategy, cyber norms and responsible behavior, cyber capacity building, and cooperation with other like-minded countries.

India issued its first national cyber-security policy[59] in 2013 which aimed at creating a safe cyber ecosystem, generating reliance on IT systems and online transactions, and enhancing the adoption of IT in all fields of the economy. Moreover, Lt. Gen. Dr. Rajesh Pant, Indian National Cyber Security Coordinator, has confirmed that the government is working on a new national cyber-security policy[60] and a draft of national cyber-security strategy,[61] and both are expected to be released in 2020.

Apart from these documents, Indian armed forces documents such as Land Warfare Doctrine 2018 and Joint Armed Forces Warfare Doctrine 2017, focused more on a paradigm shift towards non-contact warfare and stand-off capabilities as cyber to have 'decisive effects' in the battlefield. Later in 2019, the Indian government approved the establishment of India's Defence Cyber Agency (DCA), which is a tri-service command of Indian Armed Forces.[62] The establishment of DCA was suggested in 2017's Joint Warfare Doctrine to have a more focused component of defensive and offensive cyber warfare. On the other hand, Pakistan has not made public any doctrine and formation of specific cyber units.

In this evolving strategic environment, Pakistan is becoming more and more reliant on emerging technologies using online domain. Pakistan also faces consistent cyber threat in different facets such as terrorist activities in online spaces, online hate-speech, use of crypto currency, disinformation and fake news, use of cyber-attack against economic institutions and national critical infrastructures by non-state or state actors. Pakistan has been working on formulation of National

Cybersecurity Policy since 2014, but it could not be presented in National Assembly. It is high time to prepare draft national cybersecurity policy/strategy and make a clear understanding of how these threats are going to be dealt with.

In 2016, Pakistan Electronic Crimes Act (PECA) proposed the creation of National Computer Emergency Response Team (N-CERT) which would be the first responder to deal with a cyber-attack on any national critical infrastructure, but unfortunately N-CERT is not established yet. Pakistan has difficulties, mostly on political and bureaucratic level, when it comes to issues such as cyber-security, but there are ways forward. Apart from working on cybersecurity policy/strategy and N-CERT, Pakistan can work on cyber CBMs with friendly regional countries and regional organizations such as SCO, OIC and SAARC to collectively deal with the cyber threat. Moreover, Pakistan can also collaborate with its strong allies such as China and Turkey to beef up cyber defence by seeking their support.

## Conclusion

With the advanced use of cyberspace and information technology, states' concerns for defence and security are rapidly increasing. As in other operational domains, the power struggle (in cyberspace) between major states has already started to rule the virtual/cyber world for gaining maximum control.

While analyzing the above discussion, it is evident that international dialogue on information technology in the context of security has become complex. The dialogue in UNGA is highly polarized between the US (and allies) and Russia-China. Moreover, in the cyber domain, the US, China, and Russia will be the global powers in the long term with their influence on global and regional institutions and discussion. As Adam Segal predicted, it is clear that the immediate future of cyber power politics is likely to be defined on the lines of US-China rivalry. As the field of cyber and IT is still in its evolving phase, major powers

will be reluctant to agree on terms or international regulations to contain conflict in cyberspace, for at least in the near future.

With the US-China current friction, the conflict in cyberspace will only become more belligerent, and the stakes more consequential.[63] As countries are increasing their cyber military capabilities, the cyber component may not be the sole determining factor of the conflict and dominance over the adversary but, cyber-attacks may escalate the crisis between states in the future. As the cyber domain is recognized as an operational domain, with the increase in capabilities, and scope and intensity of conflict; the proliferation of cyber arms is imminent.

## Endnotes

[1] Gen. Larry D. Welch (Retd.), "Cyberspace-The Fifth Operational Domain," Accessed December 23, 2019, https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx.

[2] Cyber Operation Tracker is a database of all state-sponsored cyber-attack, initiated and compiled by Council for Foreign Relations under its Digital and Cyberspace Policy Program and Center for Strategic and International Studies (CSIS).

[3] "Cyber Operations Tracker," Accessed December 14, 2019, https://www.cfr.org/interactive/cyber-operations#Timeline.

[4] Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective," Accessed March 2, 2020, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

[5] Eric Rosenbach Shu Min Chong, "Governing Cyberspace: State Control vs. The Multi-stakeholder Model," Accessed August 29, 2019, https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model.

[6] Yi Shen, "Cyber Sovereignty and the Governance of Global Cyberspace," *Chinese Political Science Review* 1 (2016):81–93. DOI 10.1007/s41111-016-0002-6.

[7] Ibid.

[8] Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and US-China Relations," Accessed March 8, 2020, https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

[9] Dr Katharina Ziolkowski, "Confidence Building Measures for Cyberspace-Legal Implications," Accessed on April 22, 2020, https://ccdcoe.org/uploads/2018/10/CBMs.pdf.

[10] James Carafano, "All a Twitter: How Social Networking Shaped Iran's Election Protests," *The Heritage Foundation,* July 20, 2009, https://www.heritage.org/global-politics/report/all-twitter-how-social-networking-shaped-irans-election-protests.

[11] "5G Economy to Generate $13.2 Trillion in Sales Enablement by 2035," *Qualcomm,* November 7, 2019, https://www.qualcomm.com/news/releases/2019/11/07/5g-economy-generate-132-trillion-sales-enablement-2035.

[12] Ibid.

[13] News Desk, "US-China Trade War," *BBC News,* Last modified January 16, 2020

[14] Scott Bade, "How Huawei is Dividing Western Nations," *TechCrunch,* last modified March 28, 2020.

[15] Eamon Javers, "Trump official compares Huawei to 'the Mafia' as White House works on 5G battle plan," *CNBC,* February 25, 2019, https://www.cnbc.com/2020/02/25/trump-official-calls-huawei-mafia-as-white-house-works-on-5g-battle-plan.html.

[16] "Joint Pub 3-13: Joint Doctrine for Information Operations, October 9, 1998," Accessed February 9, 2020, https://www.hsdl.org/?abstract&did=3759.

[17] "Developments in the field of information and telecommunications in the context of international security," Accessed March 16, 2020, https://www.un.org/disarmament/ict-security/.

[18] "Resolution Adopted by the General Assembly on 3 December 2004," Accessed March 16, 2020, https://undocs.org/A/RES/59/61.

[19] *SIPRI Year Book 2019: Armaments, Disarmament and International Security* (London: Oxford University Press, 2019), 482.

[20] "Fact Sheet: Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019-2021," Accessed January 22, 2020,

https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf.

[21] "Developments in the field of information and telecommunications in the context of international security."

[22] *SIPRI Year Book 2019,* 482.

[23] Koskenniemi, M., *From Apology to Utopia: The Structure of International Legal Argument* (Cambridge: Cambridge University Press, 2005), 184-85.

[24] Rex Hughes, "Treaty for Cyberspace," *International Affairs*, vol. 86, no. 2 (2010): 540.

[25] Adam Segal, "From Titan Rain to Byzantine Hades," in Jason Healey, ed., *A Fierce Domain in Cyberspace*, 1986–2012 (Arlington: Cyber Conflict Studies Association, 2013), 165–167.

[26] James Joyner, "Competing Transatlantic View of Cybersecurity," in Derek Reveron, ed., *Cyberspace and National Security* (Washington, DC: Georgetown University Press, 2012), 161–162.

[27] J. Farwell and R. Rohozinski "The New Reality of Cyber War," *Survival*, vol. 54, no. 4 (2012): 23–25.

[28] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington, DC: US-China Economic and Security Review Commission, 2012), 14.

[29] David Finkelstein, "China's National Military Strategy: An Overview of the 'Military Strategic Guidelines,"' *Asia Policy*, no. 4 (July 2007): 68.

[30] Adams et al., *Occupying the Information*, 14–15.

[31] Richard Clarke and Robert Knake, *Cyberwar: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 144–147.

[32] A report issued by US-China Economic and Security Review Commission in 2012 indicates that the PRC's Military Strategic Guidelines were last revised in 1993 under Jiang Zemin, whereas a DoD report indicates that the same document was revised in 2004. US Department of Defense, *Annual Report on Military and Security Developments Involving the People's Republic of China* 2012, 3.

[33] US Office of the President, "Critical Infrastructure Protection, Presidential Decision Directive/NSC 63, May 22, 1998," Accessed March 16, 2020, http://fas.org/irp/offdocs/pdd/pdd-63.pdf.

[34] Ibid.

[35] US Office of the President, National Strategy to Secure Cyberspace (Washington, DC: Office of the President, 2003), x.

[36] US Office of the President, "Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resource, Development of Homeland Security Presidential Directive (HSPD) no. 7, December 7, 2003," Accessed March 6, 2020, https://www.dhs.gov/homeland-security-presidential-directive-7.

[37] "Department of Defense Strategy for Operating in Cyberspace 2011," Accessed March 17, 2020, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

[38] "National Cyber Strategy of the United States of America," Accessed Mach 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[39] "Summary: Department of Defense Cyber Strategy 2018," Accessed March 21, 2020, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[40] Patton Adams et al., *Occupying the Information*, 9.

[41] Desmond Ball, *Signals Intelligence in the Post–Cold War Era: Developments in the Asia-Pacific Region* (Singapore: Institute of Southeast Asian Studies, 1993), 50–51.

[42] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA*

*Missions Other Than Taiwan* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, 2009), 272–274.

[43] Department of Defense, "Joint Task Force on Computer Network Defense Now Operational," Accessed March 10, 2020, http://www.bu.edu/globalbeat/usdefense/Defenselink123098.html.

[44] NIPC is the lead federal agency in charge of protecting the US computer networks and information systems.

[45] Healey, *A Fierce Domain*, 44–45.

[46] Healey, *A Fierce Domain*, 65–66.

[47] " Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," Accessed March 25, 2020, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[48] "Congressional Research Service Report: Defense Primer-Cyberspace Operations," Accessed March 29, 2020, https://crsreports.congress.gov/product/pdf/IF/IF10537.

[49] Healey, *A Fierce Domain*, 68–69.

[50] Gu Liping, "China Hit by World's Largest Number of Cyberattacks in 2018," *Ecns*, February 22, 2019, http://www.ecns.cn/news/sci-tech/2019-02-22/detail-ifzevinw9626699.shtml.

[51] Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee, 2011), 1–5.

[52] US-China Economic and Security Review Commission, *Annual Report to Congress, 2012* (Washington, DC: US Government Printing Office, 2012), 155.

[53] *SIPRI Year Book 2019*, 482.

[54] "Global Conference on Cyberspace 2017," Accessed March 20, 2020, https://dig.watch/events/global-conference-cyberspace-2017.

[55] Global Conference on Cyberspace (GCCS) 2017, 'Chair's statement-summary', November 24, 2017, https://www.mofa.go.jp/mofaj/files/000311141.pdf; and Lea Kaspar, 'GCCS2017: A cyberspace free, open and secure (but mostly secure)', Global Partners Digital, November 29, 2017, https://www.gp-digital.org/gccs2017-a-cyberspace-free-open-and-secure-but-mostly-secure/.

[56] "Cyber Worshop Held for Shanghai Corporation Organization Delegation," The Hans India, August 3, 2019, https://www.thehansindia.com/news/cities/hyderabad/cyber-workshop-held-for-shanghai-corporation-organization-delegation-551631.

[57] "Build Asia 2019: International Exhibition & Conference," Accessed January 4, 2020, https://moitt.gov.pk/NewsDetail/YTE3NjIyOGUtODllNS00YmRiLWE5OTQtNGYwZWI3NGIxNmYy.

[58] "Closing Ceremony of International Conference on Frontiers of Information Technology-FIT 2019," Accessed January 4, 2020,

https://moitt.gov.pk/NewsDetail/Mjc3NWU3MDMtMDgwZi00MTNmLWJjYzItOTFiODNlODU2MTg1.

[59] "National Cyber Security Policy, 2013," Accessed March 29, 2020, https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf.

[60] "Government Likely to Announce New Cyber Security Policy in Three Months," *The Economic Times*, March 11, 2020, https://economictimes.indiatimes.com/news/defence/government-likely-to-announce-new-cyber-security-policy-in-three-months/articleshow/74580639.cms?from=mdr.

[61] "National Cyber Security Strategy to go for Cabinet Nod Soon: Rajesh Pant," *The Economic Times*, February 18, 2020, https://economictimes.indiatimes.com/news/economy/policy/national-cyber-security-strategy-to-go-for-cabinet-nod-soon-rajesh-pant/articleshow/74183503.cms?from=mdr.

[62] "Government Approves Setting Up of Defence Cyber Agency," *Times of India*, November 27, 2019, https://timesofindia.indiatimes.com/india/govt-approves-setting-up-of-defence-cyber-agency/articleshow/72264836.cms.

[63] Adam Segal, *Hacked World Order*.