IS CYBER DIPLOMACY ESSENTIAL IN THE PRESENT PERSPECTIVE?

Madhavji Shrestha[1]

Abstract:

It is now obvious that cyber space is the last frontier of man's research and relevant activities to empirically learn about its multi-dimensionality and its immensely huge prospect. The quest is certainly increasing each passing day. The meteoric development of information technology together with scientific development has tremendously helped to push ahead its advance in recent decades, and in particular, the advanced and developed countries of the world have steadily made their efforts in carrying out their preferred activities and to know about what lies in the future for humanity on the earth. They have, at their disposal, human resources, capital resources, and material resources with compatible managerial skills to move on toward what they have projected as their goals for their countries and citizens. As cyber space has drawn the attention of the people around the world, it has emerged as the common concern of humanity. In reality, it has touched upon human activities mainly related with scientific, technological and socio-economic domains. Naturally, diplomatic activities that regulate and act on state-to-state and government-to government relations could not remain exempt, and nor touched upon as human security, and social and economic security are closely linked together. The human security and human welfare are closely related with activities in the cyber space. As a consequence, diplomacy connected with the cyber space has now come up as an unavoidable activity, not alone in technologically advanced countries but even in all the countries of the world as humans have to live and work in their respective territorial domains. Cyber space is the common concern of all the mankind. Hence, a pressing need for cyber diplomacy

[1] Mr.Madhavji Shrestha, former Joint Secretary of the Foreign Ministry is now associated with the Institute of Foreign Affairs (IFA), Kathmandu.

is essentially felt to have its own traction that can ensure amicable and friendly relations among all independent and sovereign countries of the world. A globally acceptable convention and practice of cyber diplomacy is also required to regulate its handlings and relevant activities. This piece tries to show how cyber diplomacy has come to occupy an iconic status in diplomatic ventures worldwide with its importance growing rapidly as pushed by information technology.

Keywords: *Cyber space; Cyber activity; Cyber research; Cyber diplomacy; Cyber security.*

Introduction:

The consequential contribution of the meteoric development of information technology (IT) to the diplomatic art and practice is unmistakably the emergence of cyber diplomacy in recent decades. The term has gained its own currency and significance, and made its own traction in the diplomatic dealings across the globe. For the people of the ancient Greece, it means an art of governing a vessel in the sea induced and driven by the techniques and strategies of information governance. Currently, how this branch of diplomacy has come to be connected with the cyber space and cybernation to be operated by cyberneticians as guided by responsible diplomatic authorities as well as by private and non-state actors alike.

Although the term has been in use both in the state and non-state action areas, it has yet to gain its recognized own currency along with, which can be formulated either through the world body like the United Nations (UN) or all tech-advanced countries with a purpose to make it acceptable for and embraced by the global community. Doubtless, the term is inseparably linked with sensitive concerns like cyber security, cyber-crime and cyber espionage as well as cyber-hacking on one hand, and on the other, it is also related to national economies, scientific researches, human rights and human welfare as well as a host of national interests of the global society.

The fast-paced development of the internet and cyber-relevant technologies constitutes one of the pivotal foreign policy and diplomacy actions in these early decades of the 21st century. The potential benefits of cyber space seem numerous and boundless. In the meantime, technical threats and technical sabotages in cyber space posed by state and non-state actors have considerably increased in their sophistication, and dimension and volume simultaneously.

In our time, scientific and technological advance together with research and development in the sphere of cyber space has largely contributed to better understanding in its field. While viewing the current activities with an eye to its future development, its march toward the infinity of its contributions can ensure as much benefits as its increasing utility could provide for.

Its notable development

Man's inquisitiveness to learn about cyber space has dramatically increased when the erstwhile Soviet Union launched the world's first space-craft Sputnik in 1957 and successfully put its first human Gagarin in orbital space flight in April 1961. Finally, Neil Armstrong, the first American astronaut put his legs on the moon in July 1969 ever first in the human recorded history. Those events have tremendously raised the strong competition in the space flight race between the United States and the then Soviet Union, which had remarkably induced research activities in the space resulting in the current shape of space race as well as culminating in the application of cyber space diplomacy and its concomitant actions.

It is well-known that the space is the last frontier of human exploration and human venture with the preparedness and tech- savvy available at the disposal of advanced and developed countries with fierce competition to win over the targeted rival against each other. Its resultant effects could affect international relations with likely repercussions in the relationships between influential and powerful countries. In turn, that would prevail over the international community involving even smaller and weaker countries. Hence a compelling need for cyber diplomacy is inherently felt all over the world, both advanced and less advanced included, depending on their technological capability and willingness to forge ahead in the targeted direction of their choice with apparent importance attached to the alliance of their preferential priority.

The current global situation demands that super and major powers should envisage cyber diplomacy as an inherent opportunity to provide another strategic platform for global connectivity. That is, however, easier said than done in actuality as the world today is too divisive with intense conflicts of national interests gaining ground conspicuously. The Russia-Ukraine war since February 2022 has amply demonstrated the emerging trend-setting in the context of narrower national interests and flaunting their prowess in the external dealings with priority significantly attached to the domestic needs both economic as well as strategic interests primarily preferred by respective governing clique at the helm of the state power.

In recent time, experts of diplomatic practice with a constructive bent of mind are in search of art and tools to find strategic and situation-compatible approach to get started with the acceptable traction in both maintaining strategic balance of relationships in existing troublesome dealings among the states in conflict of national interests. However, it must be stated that no easy way of finding solution to problem / problems existing between nations, and more so, in case of those states and governments whose borders are closely linked with each other. The question of borders along with the border dwelling peoples has come up as the unavoidable concern of contention between states. More often, the conflict situation emerges where there appears the greed for valuable natural resources, which has now been playing out as primary concern for big and non-amenable difference between nation states. This undesirable trend-setting has to be arrested if the world is to be made a live-able place for humans who aspire for the march toward continued progress and prosperity. Considering the knowledge obtained by scientists and experts the planet of Mars is most likely to become habitable for humans as the continued exploration and deeper research done by the United States and China in most recent years demonstrate that the planet Mars may become habitable in the years to come. However, that will not happen in the near future.

The relentless exploitation of natural resources both above and beneath the template of the earth has its devastating impact on our planet coupled with climate change effects all around. Humans both being rational as well as caring social beings must see the futuristic prospects in their proper perspectives. Space being the last resort for human activities together with the prospective for immense future promises can ensure for the mankind to move forward for its befitting survival and undisturbed journey in several eons to come. The progress and prosperity achieved through the ingenuity and human effort since the early 19th century to date have changed the face of the earth for betterment of human well-being. Of course, the path to the unprecedented development is not without its adverse impact as well. Humans have to become more sensible and rational if any achievements have to be made by walking through the charted and uncharted trajectory that can encourage and induce diplomacy primarily intended to bring about its use in channeling through the cyber space that would enable both state and non-state actors to adopt and adapt upcoming cyber diplomacy. Its importance now looks impressive and its utility pervasive. Its future is shining and in the meantime, promising to render useful services to all the countries and peoples of the world with each moment around the year.

Defining cyber diplomacy

To move on for clearer understanding of this newly emerging cyber diplomacy, it would be useful to ponder over some of its definitions as offered by some well known experts. It would be pertinent here to quote here some of them, which run: "Cyber diplomacy is broadly defined as the use of diplomatic tools and initiatives to achieve a state's national interests in cyberspace that are commonly crystallized in the national security strategies (Manantan 2020). "Cyber diplomacy can be defined as diplomacy in the cyber domain or in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interest with regard to the cyberspace. Such interests are generally identified in national cyberspace or cyber security strategies" (expert). Some more definitions need to be cited: "Cyber diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests are generally identified in national cyberspace or cyber security strategies?" (Christian 2019). Finally it is appropriate to quote one more definition. It states; "Cyber diplomacy is defined as the use of diplomatic techniques and the performance of diplomatic tasks by governments, organizations or individuals in cyberspace to protect their interests" (Ziegler, 2023). All definitions quoted in the foregoing lines point out the most sacrosanct duty of serving and promoting the national interests of each state. The only difference is that cyber diplomacy is carried on and activated through cyberspace unlike under the conventional diplomacy performed through the offices based on political capitals. However, cyber diplomacy is applied in all or in part by assigned diplomats, meeting either in bilateral forums or in multilateral forums. Besides all that, diplomats also interact with various non-state actors, such as executive bosses of the internet companies, technology entrepreneurs, civil society organizations etc. This new stream of diplomacy requires an additional skill of handling necessary affairs of diplomatic domain with adequate training on internet and information technology. Efficient handling is a 'must' to effectively conduct cyber diplomacy. If not, it may bring chaos and confusions. Such probable situations are not liked by anyone, nor could that enable anybody to contribute anything concrete. Strategic management donned by well-trained personnel and supplied with adequate resources is indeed the primary situation that can create an environment for successful performance through cyber diplomacy which is being fast pushed by the rapid development of information technology now. The practical use of cyber diplomacy has now emerged as one of emerging factors in the conduct of the ultramodern diplomatic businesses that has come to stay as an irreversible trend.

Main functions of cyber diplomacy

In recent decades, the rapid development of information technology and internet has come to contribute an integral part of the foreign policy formulation and its execution. In fact, cyber diplomacy is the pinnacle of such fast development of diplomatic business. It is, therefore, very important to have a closer look at main functions of cyber diplomacy. Let us see what an expert has enumerated following functions (Painter, 2018) as enunciated by him:

1. Building strategic partnerships and engaging multilaterally
2. Enhancing cooperation, collective action, incident response and capacity building
3. Advancing strategic policy and building consensus for global cyber stability
4. Deterrence
5. Mainstreaming cyber issues in the development process

Another expert on the subject describes the following functions (Ziegler, 2023):

A. The formation of dialogue and communication between state and non-state actors

B. The collective response to cyber threats

C. The non-proliferation of cyber arms

D. The advancement of national interests in cyber space through diplomacy and cyber security policies

E. The protection of human rights in cyber space

F. The development international cyber laws

From above two sets of functions as offered by the two experts, we can conclude that multilateral and global cooperations stand as an essential ingredient to proceed toward the actual conduct of cyber diplomacy. Only on that condition, it can work properly without any hitch.

No doubt, cyber diplomacy is emerging fast. It has now appeared unstoppable in the past one and half a decade i.e. since 2007. However, the development has also faced some challenges that need to be practically met for its normal operation. An expert on the emerging aspect of challenges has enumerated following challenges (Ziegler, 2023)

- The reluctance of states to participate in cyber diplomacy
- The rapid growth of cyber technology
- Cyber diplomacy creates a political divide among states.
- Questioning the legitimacy of international law
- Cyber diplomacy preserves the interest of non-state actors

The rapid evolution of cyber technology has indeed brought in awkward situation of confusion and chaos in the present global and international order, because it has not yet assumed globally recognized standard, nor enacted rules to be followed by the international community. In the absence of such accepted standards and rules, misunderstanding and wrong communication may naturally take place. Under such circumstances, undesirable disadvantages and disruptions might appear to the detriment of national and global interests of various dimensions. The challenges coming out of this latest technology of the cyber space, therefore, need to be primarily grasped and clearly understood to put it in an agreed array.

The fast-paced development of relevant technology closely related to the cyber space has indeed colonized the entirety of the planet earth, never seen before its advent under the development of any civilization around the globe. It is, indeed, the gift of great ingenuity of humans and material facilities available mostly in the economically advanced and technologically better off countries.

Cyber security threats

Often, the user faces security threats while in work at the public or private place. The user, whether be an individual or group or state is required to understand and bear responsibility for non-disrupting works. He may face threats like cyber hacking, cyber theft, cyber disclosure, cyber disruption or any other disturbance etc. To work in an efficient manner to obtain desired outcome, the user must understand cyber threats and vulnerabilities posed by the negative mindset and disruptive behavior of individual or state actor. Threats are several in number, but some experts have identified six sorts of them (cyber security best practices, 2021), which are enumerated below:

1. Phising – A malicious individual or organization may 'fish' for information by using communication, such as emails, to try and gain login credentials or other sensitive information

2. Malware – Malicious software designed to perform an attack on the device or server that down loads or runs it.

3. Ransome-ware – This is a type of malware that essentially looks down a victim's files, encrypting them so they cannot be assessed.

4. MITM- when expanded this explains a man-in-the middle (MITM) attack is when an attacker establishes a position between the sender of a message or information, and the recipient, allowing them to intercept any correspondence.

5. Trojan – Trojan viruses are other forms of malware

6. DDOS attacks- A denial of service distributed denial of service attack (DDOS) occurs when a handler uses multiple devices (often numbering in the thousands) and uses them to overload target system.

Additionally, the threat of cyber security in general may also come under various forms of attack, for example, network security attacks, wireless security attack malware attack, social engineering attack depending on the choice of attack.

The user, whether individual, group or organization needs to realize that no system is perfect or hundred percent vulnerability-free or "hacker proof" The threat committer may have enough time, necessary resources and sufficient manpower to commit an attack. He will find chance or chances to commit his misdeed with the way he finds easy.

Knowing well in advance some potential threats to the cyber security, group or organization maintains and monitors the defenses of a network and its system while other group or organization of evil doers stimulates real attack in an attempt to break into system either externally or internally. As a consequence, companies gain a better understanding of various types of threats that exist to pose toward their functioning system. In reality, the most robust and effective security system will have a continuous and real-time level of defenses such as security operation centre (SOC) managed detection and response (MDR) or active threat.

Hunting and analysis

It is to be noted that threat groups exist everywhere. Cyber attacks happen in all shapes and sizes from deploying an application specific attack against a data base server, posing disruptions and damage even at the time when it is most needed for the active performance of cyber diplomacy. One notable quote from the well-known diplomat of the United States states: "Serious study on the problem from the information technology is needed to face off with challenges originating from this fast and uncontrollable development. Nation-states could not be blamed for this particular development as even a tiny group of talented people could emerge effective imposing serious threat" (Haass, 2017)

This newly emerged practice of cyber diplomacy is considered as strategically central to the use of "global common" as no powerful single or a group of the powerful would not be capable enough to protect various segments of national interests ranging from highly secretive security interest, economic interest to the maintenance of privacy and freedom of citizens. Unified approach and strategy sustained by trust and confidentiality of each other is essential.

One important quote will further clarify: "To respond to cross national cyber attacks" and harmful acts, for example, states must extend cooperation in "information sharing evidence collection and criminal persecution of attack perpetrators". In fact no state can single-handedly protect itself against cyber threats". (Khabbaz, 2021)

Notwithstanding encountered as well as presumed threats, the current application and conduct of cyber diplomacy is indeed on the increase on the global scale. Some global efforts could be cited. In 2004, the "UN General Assembly instituted the UN Group of Government Experts on Development in the Field of Information and Telecommunication in the

Context of International Security (UNGGE)". In its report made public in July 2015, the adoption of international cyber norms and international cooperation and communications technology (ICTS) were discussed. But UNGGE negotiations met failure during the June 2017 session of the group.

In September 2019, 26 countries issued a joint statement at the UNGA on the norms of cyberspace. The signatories in this statement included the United States and European countries. No other countries seemed willing to become signatories as their national interests are hardly likely to be met by provisions contained in the statement. Non signatories happened to be most countries of Asia, African and Latin America which are either at the developing status or the least developed ones, especially in the field of cyber related technology and its relevant branches of utility. All that occurred in the pre pandemic years could not make any breakthrough on any of remarkable successes but they made some footprints in the realm of preventing cyber threats to ensure protection from cyber threats.

With the unprecedented of development of information technology, have come various threats before the user whether he be an individual or group or the state organization as discussed above. Information technology has now become an integral part of the human life around the globe. Its benefits are abuzz with its growing importance. Hence, experts have also developed protectionist measures. One of well-known experts, Mathieu Chevalier of Genetec Inc. of Canada has developed at least 5 steps to help the user / users for the safe handling of IT and its relevant uses. He has offered 5 steps as listed below.

1. Learn how to detect a potential social engineering attacks

   This first step requires from handlers of computer system their personal credential, financial information and personal information along with their links and files as well as their suspicious phone calls.

2. Educate users and devices

   Refraining from using third party applications that have not been approved by the IT department is also a key factor.

3. Implement multi-factor authentication and password management

   Password management policies and multi-factor authentication (MFA) are essential when it comes to securing devices. This is crucially important to protect cyber security.

4. Keep up with the best software and hardware practices

Software and hardware physical security with best practices help to ensure that the user is doing all he can to secure his organization. And products updates often provide critical fixes for new found vulnerability.

5. Choose the right technology

   Selecting the right technology is pivotal to a strong cyber security, as operating with transparency and maintaining clear and correct communication around vulnerabilities allows the user's organization to create an optimal cyber security strategy.

Cyber security best practice is an endless process while it begins at on-boarding, both new and existing employees require constant remainders and updates on the steps that they must take, every day to protect the organization against an evolving numbers of cyber threats.

In addition to the above 5 steps, another expert David Bianco has offered 10 ways to protect cyber security from different systems and quarters. They are as follows:

1. Security policy first
2. Don't neglect physical security
3. Screen new hires
4. Use strong authentication
5. Secure desktops
6. Segment LANs
7. Plug information leaks
8. Investigate anomalous activities
9. Refocus perimeter tools and strategies
10. Monitor for misuse.

Generally considering, the organization can safely employ these as a matter of policy for all employees, using information technology at the computer system.

In the meantime, it is essential to keep the computer system and applications updated. There is also a need to avoid links, programs, devices and attachments from unknown sources and unfamiliar visitors.

Need for training of cyber security

Values and norms of practical trainings assume greater importance for normal and smooth functioning of the computer system. Timely and appropriate trainings for employees would lie at the root of minimizing security threats. Good trainings imparted to employees would adequately pay off to the organization. Experts suggest the following topics for trainings to be imparted to employees who diligently work for the organization.

1. Cyber security operations
2. Cyber security foundations
3. Start building the employees career in cyber defense
4. Digital security training
5. Digital security design and development
6. Network defense management
7. Introduction to cyber security
8. Introduction to cyber security for teachers

It needs not be much emphasized that everyone using the computer system for cyber diplomacy can benefit from some basic cyber security training and with a range of micro-credentials, courses, and expert tack, the user can soon start mastering this crucial skill. The trainings are basic requirements that would confer benefits and required skills on both the organization and its employees institutionally and individually.

The 21st century has both profusely and profoundly witnessed an extensive application of information technology in the areas of both individual and national life with its unprecedented development. It has entrenched almost all shades and dimensions of human life in an undeniable way. Now there arises no question of going back from its ever expanding application. Indeed, it has gained deeper and wider significance in human life. It is also expected that its meteoric progress at the moment would certainly keep transforming the shape of the world in not too distant a future.

Nepal's status in the perspective of cyber diplomacy

In general, people keenly interested in cyber diplomacy have rarely heard about Nepal's cyber diplomacy in action. It is not yet even in its infancy in Nepal. But the pressing need for it is being felt as cybercrimes and cyber espionages, cyber thefts etc. are reportedly on the increase. To be on the safe side, decision making authorities need to be carefully circumspect and ever vigilant in initiating reliable steps to put cyber diplomacy on its track. Various media reports have it that Nepal has in the past enacted the Electronic Transactions Act 2006, Nepal Information and Communication Policy 2015, Digital Nepal Framework 2019 and so on. All those Acts and relevant regulations might become an embryo of cyber diplomacy. Hence, forward looking with strategic acts and actions to place Nepal in the interface of fast accelerating cyber diplomacy across the globe would be helpful to put it on track. The Kathmandu Post of July 3, 2021 in its column described that Nepal has moved up to the 49th position in the global cyber security in 2020 from the 106th slot in the 2018 edition, showing that its commitment to cyber security has increased, according to the International Communication Union (ITU). According to ITU, Nepal scored 44.99 out of 100 points among 182 countries of the world. It was placed 17th among 18 countries of the Asia-Pacific region.

Globally, the United States topped the chart scoring 100 points, followed by the United Kingdom and Saudi Arabia with 99.54 points each. In South Asia, India topped the list in the global cyber security index scoring 97.5,

Nepali media has it that the Ministry of Communication and Information Technology had prepared a draft National Cyber Security Policy 2021 to control and minimize cyber attacks in information technology and provide security from possible future attacks. As of mid-May (2021) 90.56 percent of the population of Nepal had access to the internet. The number of internet users in the country stand at 27.37 million.

On May 2, 2023, the incumbent Minister for Communication and Information Technology of Nepal had expressed the commitment of the government for cyber and data security on the occasion of the National ICT Day, during which the Chief Secretary of the Government of Nepal had emphasized the need to provide reliable and equitable access to IT to ensure inclusive prosperity (Rising Nepal, 2023)

Succinct discussions above have shed some light on the cyber realm and cyber activity in general. However, the main concern here is the conduct of cyber diplomacy that has emerged to occupy the position of compatible and comfortable process of the recent adoption of diplomatic activities., To walk on fairly with the embrace of the recent practical trend, there is a need to put up essential mechanism equipped with meticulously trained and highly skilled manpower. Also, no need to mention here that the Ministry of Foreign Affairs of Nepal together with the close cooperation and assistance of the Ministry of Communication and Information Technology as well as other relevant Ministries of the Government could proceed to put in place the launching of cyber diplomacy that has been embraced as a reliable process of handling diplomatic affairs by advanced countries of the world and big power of our South Asian region alike. Certainly, cyber diplomacy has conferred benefits and facilities on its users, which have been proved useful even during the recent complex diplomatic dealings, because the conduct of cyber diplomacy is now appearing safe with possible threats largely removed from the scene, but not yet eliminated completely. Threats still exist from the individual, group or even state actor.

It may be, however, noted carefully that for the safe and smooth handlings of cyber diplomacy, need for the installation of good hardwares and soft- wares of internationally branded companies are very essential. And employees handling those wares should be honest and dedicated with the sense of and devotion to the sincere duty toward the institution which has employed them in view of serious challenges and imminent threats as highlighted in the foregoing lines. Nepal must not lag behind in conducting cyber diplomacy as it is being adopted and adapted by prominent countries of the world. The feeling and attitude of less developed status need not be a barrier. Forward Nepal must to stand in the interface with the other countries of the global community.

Experts of cyber diplomacy recommend to any user institution to employ reliable averters who are well trained on the subject to control and prevent any disturbance and disruption frequently committed by saboteurs, hackers, wrong-doers, etc. No need to worry, if wares and devices were installed in a technically sound way by meeting accepted international standards and if users perform their duty with sincerity and devotion

References

Attatfa, K.R. et al, 2020, Cyber Diplomacy; A Systematic Literature Review (Vol-176, 2020, pp 60-69)

Budapest Convention on Cyber Crime, 2001 Council of Europe, European Treaty Series no.185

Cacacho, M. 2021, Cyber Security Policy in Developing Countries, Rowing in an unfamiliar world without a paddle.

Chevalier, M. 2021, Genetec Inc. Montreal, Québec, Canada.

Cyber Security Policy 2021, Kathmandu, Nepal

Digital Nepal Framework 2019, Kathmandu, Nepal

Erstad, W. 2022, 10 Cyber Security Problems Nearly Every Organization Struggles with, Rasmussen University,

Five Easy Ways to Protect from Cyber Attacks, 2022 Victoria University, Melbourne, Australia

Haass, R.N, 2017, The World in Disarray, Council on Foreign Relations, New York. USA

Information Technology Policy 2010 later revised as Information and Technology Policy 2015, Kathmandu, Nepal

Khabbaz, D. 2021, Cyber Diplomacy, Benefits, Developments and Challenges

Manantan, M.B.F. 2021, Defining Cyber Diplomacy, Australian Institute of International Affairs, Australia

Norwich University Online, 2020, The Increasing Need for Cyber Diplomacy, Norwich, United Kingdom

Painter, C. 2018, Diplomacy in Cyberspace, The Foreign Service Journal, U

Salem, E. MD, 2020, A New Battle Plan for Defeating Cyber Threats

The Cyber Diplomacy Act 2017, Washington, USA

The Kathmandu Post, July 3, 2021, Kathmandu, Nepal

Threats to Cyber Security, 2023, University of North Dakota, USA

Access this article online

www.ifa.gov.np/www.nepjol.info

For reference: Shrestha, M. (2023) Is Cyber Diplomacy essential in the present perspective?

Journal of Foreign Affairs (JoFA), Volume 3, Issue 1

DOI: https://doi.org/10.3126/jofa.v3i01.56501