Global Cyber Diplomacy in the era of Network Centric Platforms

Alok Vijyant*, Dr J.S.Sodhi**

The cyber domain pervades modern societies and is constantly evolving. A lack of mutually agreed upon rules of the road poses a challenge to stability. The international community has yet to develop a common understanding of what constitutes a norm violation, which specific categories of targets should be off-limits to certain types of cyber operations, and so on.

Extensive research has been done on cybersecurity, cyber-politics, and security in the digital age (Valeriano, Jensen and Maness 2018). The impact of these developments for the international order, and diplomacy as a potential complementary practice to the security-oriented approaches, has however remained largely unexamined in the literature .

Cyber diplomacy has thus emerged in response to a demand for an approach, which centres around promoting peaceful relations in the international system. Core challenges of cyber diplomacy is how to create international order out of a largely anarchic domain and establishing the necessary conditions for intergovernmental cooperation to increase cyberstability (Attatfa 2021; Manantan 2021). The political prioritisation of this approach is illustrated by the allocation of significant resources to the creation of cyber diplomats, in addition to strategies for international engagement on cyberspace (Creemers 2020 ; Israel Defense 2021).

Several cyber governance studies have been devoted to examining the feasibility of regulating cyberspace, including through the creation of cyber norms (Finnemore and Hollis 2016), in addition to individual states' efforts towards establishing regional norms for cybersecurity Other noteworthy contributions include Nye '(2014) in a neoliberal institutionalist paper on the regime complex for governing cyberspace (2014). Particularly the UN has been the subject of several studies.

Furthermore, several case-studies of cyber powers stances on global cyber governance have been undertaken over the years, including of Russia, China, and the US (Kiggins, 2014; Nocetti, 2015).
In a literature review of cyber diplomacy by Emilie Berthelsen and Johan Doré Nellerod , Department of political Science, University of Copenhagen in their thesis covering the period of 2010-2019 found 21 scholarly articles and books on the phenomenon, with the majority being published within recent years.

.* Research Scholar, Amity Business School
** Professor , Group CIO, and Sr VP , RBEF, Amity Group.

Though few references are available in open source that talks on the setting up of stage for a network centric warfare, yet no authentic reference is available to see how the platform centric battle space is converted to a network centric platform. This paper is an attempt to provide a generic model of cyber warfare strategy drawing out of my experience in this field. The model is a thought-provoking model and does not rest its assumptions on any policies and procedures of any government of the world. It would deal with the opportunities that the nation states or the non-state actors would have in terms of exploitation and misuse of such network centric platforms.

There are three important aspects in such exploitations:
(a) How to do it ?
(b) When to do it ? and
(c) Against whom to do it.

Though, the first deals with the technical aspects of the subject, the latter two deals more with diplomacy than technology. The model presented here deals mainly with the diplomacies. The brilliance of warfighting is best exhibited through winning a war without fighting it. A good strategy of such war fighting therefore attains significance in the current world order. The tenets of such strategies must draw out from the domains of negativities as well as the technological advances.

The 9-Cell Matrix Model distinguishes the strategic stances on parameters such as – relationship with the country and the state of cyber preparedness of the country for which the stance is to be adopted. The aim is to attain dominance in the cyber battlefield with maximum number of allies made through any available methods and alienate the enemy in space. This would mean increasing one's area of influence in the green domains of cyber defense supporting economy and commerce and creating a deterrence through deployment of cyber offence and covert operations.

While giving the hypothesis on the strategy a few assumptions have been made – (a) There is no real time sharing of information among nation states, typically so when it involves multiple countries in a single instance, (b) There exists no world convention in this domain and different countries have different definitions, assessment and appreciation of cyber space, including laws governing the same, (c) There is no geographical boundaries and Internet follows the paradigm of free and smooth flow of information across, (d) No Information Infrastructure is full proof that is deployed and could be subjected to attacks of various dimensions, (e)People trust Internet for information and there exists a risk of misinformation propagation.

Cyber Stances

The cyber policy stance that a country would involve in as against another nation state could be of three types –

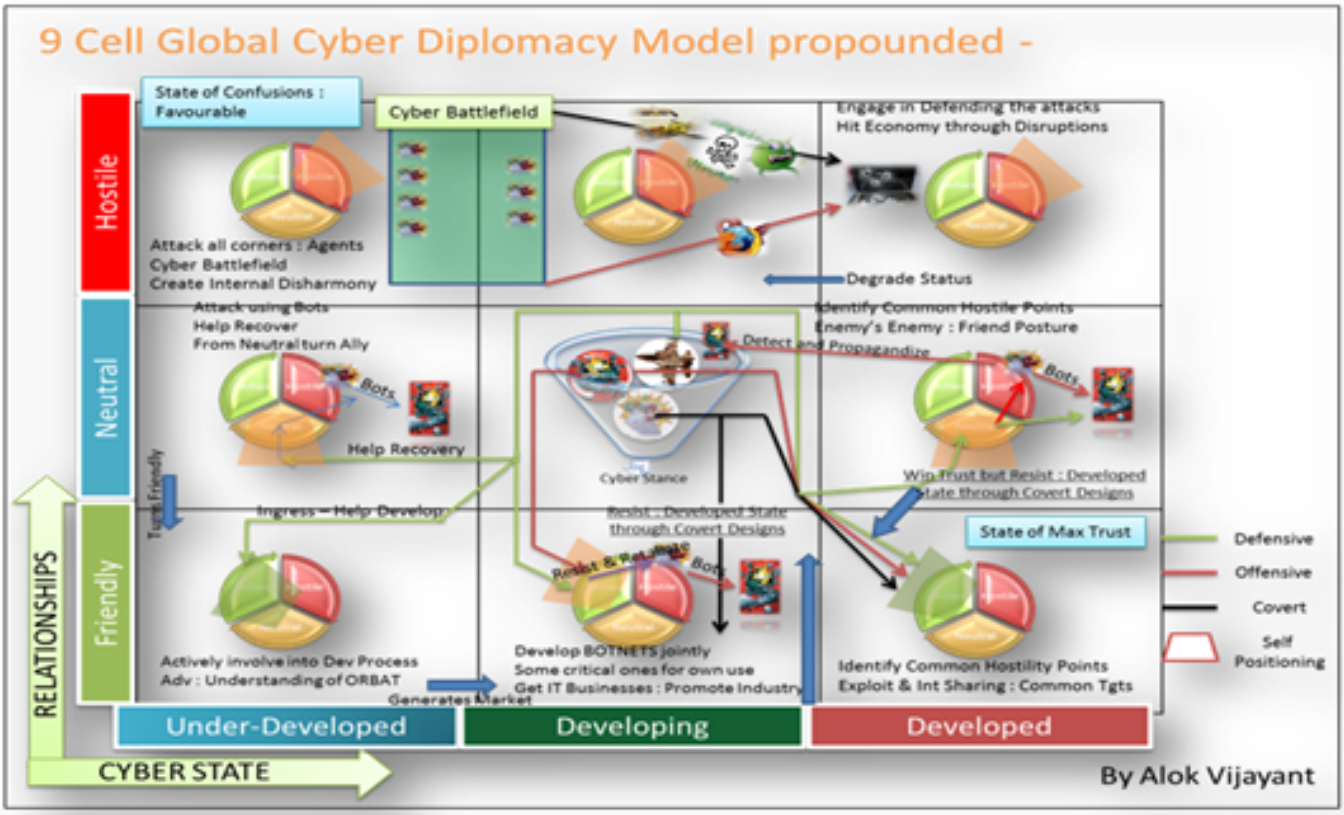
(a) **Cyber Defensive Policies** – Cyber Defence primarily focuses on guarding mechanisms that a country would adopt to protect and preserve its critical information infrastructure against any attacks by its adversary. This would involve development of tools and techniques of protection.

The areas of research could be in the software, network, protocols, hardware, and embedded systems. The defensive policies would necessitate a harmonical relationship with the freelance researchers, industries, and academia. Innovation is the key to success while adopting such policies.

(b) **Cyber Offensive Policies** – Cyber Offensive policies are pursued in order to create deterrence in this domain. The "Offensive Defence" is one strategy that is adopted to understand ones weaknesses from the enemy's perspective. It also instills a fear of retaliatory action in the adversary's mind. "No first use" kind of syndrome sets in this domain and "Cyber Non-Proliferation Treaties" would subsequently be a part and parcel of the global cyber world order.

(c) **Covert Cyber Operations** – Covert Cyber Operations are stances that are not declared by any nation state but are pursued to create conditions congenial for development of the cyber commerce. These stances are also adopted for getting to know what is not easily available as a free knowledge society. Several obscene words revolve around this stance including "spying", "espionage", "cheating", "stealing", "frauds" etc. All these activities for leveraging one's agendas are used during these operations. Since the activities revolve around dirty tricks, ensuring that such activities are not attributed to a nation as a stance is very important. Thus, no nation that would involve itself in such acts would ever try to leave traces of its involvement in that act. He would ensure that it is attributed to somebody else rather than himself.

The three stances are not mutually exclusive but operate in close coordination. The paradigm on which the above hypothesis rests draws out from "Drugs and the Arms Mafia" mode of operations, wherein demand is artificially created for growth of such businesses. One sophisticated weapon in the hand of a terrorist generates an exponential requirement of similar weapons by Law Enforcement Agencies. Thus, as the drug lord would operate – The covert channels would distribute free dosages of drugs and only to disappear later, so that the demand is created, and the supply side could extract obnoxious and super normal profits through manipulations.



Description of 9-cell model on Global Cyber Diplomacy:

The diagram looks a little complicated but the sequential explanation of the same would clear out the concepts. The positioning of a nation and its stance towards other nations depends primarily on two very important factor – the strength of respective nations in terms of cyber capabilities and relationship with other nations. On the X-Axis of this matrix, we have plotted the strength of a nation in terms of its cyber capabilities – Under-developed, developing and the developed and on the Y-Axis the relative relationships of a nation vis a vis other nation – Friendly, neutral, and hostile is plotted. The three cyber stances referred above shall be aptly applied to set the stage for a cyber-diplomacy. The aim would be to align all allies and isolate the enemy. In addition to it, the model also attempts to have diplomatic underpinnings in line with the requirement of the commercial and trade considerations.

The Defensive cyber operations would primarily aim at synergizing their acts through a Public-Private Partnership involving academia and research establishments. The directed research would lead to development of products that could have international acceptance in the current scenario. There would also be a need to find the right market for the products thus developed so that the commerce and trade can step in at the right time. The old theories of economics do suggest that the largest markets for products have been observed in the developing economies and the same theory would hold good in the current scenario too. The only lagging question to be answered is – how one would compete with other products elsewhere, after all the asymmetry in this domain would render all equal and all having the same or similar product to offer.

Thus, it would be very important to have the exact answer to the problem that is posed. A smart way of addressing this issue is to set the question yourself and answer it aptly so that ambiguity is eliminated. So, instead of problems coming in front and thereafter trying to solve it, a smarter player would create problem and solve it. The role of covert or the black operations would then come to fore. Black Covert Operators would spring into action and create an attack threat keeping in view various socio-political equations in mind. The most obvious issue catching up that nation would be capitalized and the nation engaging would be pivoted upon to create the attack vector. Once the attack vector is created, the media warfare needs to be launched with specific leakages cornering the nation that has been pivoted upon. Such media releases would help form an opinion against the nation engaging into conflicts and would immediately create a new market for products that can handle the threat vector adequately and aptly. This is the time when once again the defensive cyber operators would move forward subtly and offer the products already developed to handle the crisis to the nation where market is sought. Parallelly, the covert black operators would slowly withdraw their attack thread and give the impression that the product offered by the defensive teams have started working and are proving to be effective. This would set in a regime of trust between the two nations and at the same time the security products developed by the defensive teams in association with the industry and academic partners would be sold to the market.

Various aspects and stances that one would adopt while dealing with relevant quadrants are given as under:

Neutral-Under-Developed – There is no leverage points in the current scenario for a diplomatic underpinning. The need must be created in this stage wherein a situation is created for the country, which forces it to seek external help as a readymade immediate solution. This is the time; a defensive arm must extend support and win trust in the domain. The covert division would create an artificial crisis through mounting of attacks using Zombies spread over countries that have hostile relations with the neutral country that needs to be won over. This provides an opportunity to curtail the artificially generated attacks and gain significant trust converting a neutral nation – a friendly nation in this domain.

Friendly-Under-Developed – The neutral country that is now converted to a friendly nation needs to be supported through injection of technology and deployment of information systems at competitive rates or even free of cost. This has dual advantages – (a) You have a readymade mechanism of mapping the Information Infrastructure that is most authentic and eliminates wasteful, non-verifiable exercise of creating an Orbat and (b) The Defensive Industry grows through selling of the second rung of technical solutions. Gradually, the nation converts itself from Under-Developed to Developing nation.

Friendly – Developing – With the deployment of Information System through the green-channel approach, a stage is set to take the relations further into the offensive domains. The demand is again required to be generated artificially at this stage. The countries hostile to the country needs to be used for once again carrying out espionage related activities and the activities uncovered by the Defensive arm. This further takes the trust level to a higher level and at the same time the friendly-developing nation generates an appetite for such espionage and offensive operations. This time the offensive division becomes an automated choice with definite leverage points. This time adequate business processes could be activated to make super normal profits for the supportive industries and at the same time become a partner in intelligence and offensive operations with knowledge available for exploitation. During such joint operations, systems must be exploited that are of common concern and at the same time ensure that covertly some actions are performed for one's own usage. Care must be taken at this stage to resist the migration of this nation state from the developing to the developed nation state through frequent mounting of covert cyber operations, which would ensure persistent demand for cyber products. The advantages lie in the differential power and not on equal status.

Friendly-Developed – This is the stage of maximum trust level, wherein activities must be performed with utmost level of confidence. Since there are definite mutual strengths, a synergic situation should be developed. Common interests points must be identified before the start of any activity both on the Defensive as well as Offensive platforms to avoid conflicts later. Common hostile entities would be dealt with jointly and collaborative intelligence framework would be set up. A state of information sharing would surface.

Neutral – Developed - It is difficult to make a headway in such situations as any amount of defensive help extended would be resisted by already existing mature domestic suppliers. In such a case, the ice has to be broken using Psychological and cognitive dimensions. "Enemy's enemy is a natural ally", is a buzz word in this situation. People in similar distress become natural collaborators. An espionage attack or an offensive attack would need to be simultaneously planned. The attack would then be detected and propagandized, disclosing the source of attack. In this case, one would require to dispense with its own covert offensive resources even. The attack thread detected by the neutral-developed nation would also analyze the attack to be of a set source. Thus, a stage is set wherein the two are in similar conditions leading to a natural collaborative framework.

Hostile-Under-Developed – Such nations would be used as the cyber battlefield for parking of weapons and launch platforms. Nations being weak would be exploited with sleeper cells (Zombies). A state of confusion prevailing, is an ideal situation for development of the battlefield. A state of disorderliness would be created through ethnic Botnets, regional botnets and diplomatic botnets.

Hostile-Developing – Such nations would also be the next gen cyber battlefield and would be treated in the similar way as hostile-under-developed nations. The zombies placed on the hostile under-developed and developing nation would be utilized to attack the Hotile-Developed nation on a persistent basis. This would degrade the status of the nation and cause economic losses.

Case Study 1 : Cyber Attacks on Estonian Computer Systems

A wave of attack was witnessed on Estonian computer systems in 2006 bringing the information infrastructure to a complete standstill. The event was seen as the first state sponsored cyber-attack in the world.

Assumptions : Russian Government was behind the attack as Russian IPs appeared during the attack.

Counter Argument : With the availability of various Obfuscation techniques and false flagging mechanism, normally state sponsored activities should have been adequately covered. Russians have been known for their reverse engineering skills and are very unlikely to have made such errors.

Beneficiary : Business activities in the cyber domain of many of the developed countries witnessed a sharp rise in Estonia after the attack.

Case Study 2 : Symantec Poor Quality Control updates for Windows XP Chinese Beta Version

Symantec released certain updates in 2006 for Windows XP Chinese Beta Version that resulted in quarantining three important files of Windows system required for logging into the system both on disk and through network. The number of affected system in China touched almost a million. Symantec quickly announced payment of compensation to all the affected systems. There were only 7000 registered users of the said Operating System in China.

Case Study 3 : Attacks on Indian Information Infrastructure in 2009-10

Waves of Cyber Attacks were detected in India in 2009-10. Most of the attacks detected, provided clear indication of a Chinese footprint. In the later attacks, the Chinese footprints were “ensured to be visible”. Following the attacks, there were a number of delegations visiting from the western world with security products lined up. Is it that they were waiting for a disaster to happen and then seek business opportunities or a self-created demand? Security Researchers with known ties with various security and intelligence agencies flocked in numbers propagating Chinese involvement in anything and everything that happened to us. Some of these persons even attributed the failure of INSAT 4B power module to the STUXNET worm propagated by “Chinese”.

Case Study 4 : “Shadow in the Clouds” Report

Shadow in the Cloud report released by the Shadow Foundations and the Munk Center in April 2010 spelt out how the Chinese hackers engaged themselves in various hacking activities and pilfering sensitive data from the sensitive government systems. It also made reference to a method called “DNS Sink holing” for identifying the sensitive systems compromised by Chinese. The method necessitates a control on the mother DNS Server responsible for converting the malicious domain name to the IP Address and vice versa. The malicious domain name was sink-holed in the extant case to an owned server and was analyzed to detect the breach. Method is fine enough with a caveat – It must have support and knowledge of the LEAs or the Governmental frameworks. The question arises as to why the same method was not used to sink hole the domains of Wikileaks that supposedly brought in embarrassment to the US Government.

Conclusion

While on one hand, the network centric warfare is characterized by cross integration of various platforms and effective, reliable and secure communication among its components, it throws open a vast area for exploitation if any of its component develop a snag – both accidentally or deliberately. The weapons of this domain are easy to create, and players do not have an entry barriers to this domain. Distinctions between state sponsored and non-state actors have blurred due to the asymmetry attached to this non-traditional battlefield.

As regards the model propounded, it is my prediction that the information battles of tomorrow would be fought at the communication backbones of African and Latin American countries. A state of confusion and enhanced entropy would be the success milestones in this domain. Cyber Warfare Management and Control would form one of the larger and much sought-after disciplines of management.

References

Attatfa, A. (2021) 'Cybersecurity: a pillar of Cyber diplomacy', Le Journal International.

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

Kremer, J.-F. and Müller, B. (eds) Cyberspace and International Relations: Theory, Prospects and Challenges. Berlin, Heidelberg: Springer, pp. 161–180. doi:10.1007/978-3-642-37481-4_10.

Israel Defense (2021) Blinken presents the foundations of U.S. cyber diplomacy,

Finnemore, M. and Hollis, D.B. (2016) 'Constructing Norms for Global Cybersecurity', The American Journal of International Law, 110(3), pp. 425–479.

Nye, J.S. (2014) 'The Regime Complex for Managing Global Cyber Activities', The Centre for International Governance, Global Commission on Internet Governance (Paper Series No. 1), p. 32.

Kiggins, R.D. (2014) 'US Leadership in Cyberspace: Transnational Cyber Security and Global Governance'

Nocetti, J(2015); Contest and conquest: Russia and global internet governance ',International Affairs , 91(1), pp 111-130

Emilie Berthelsen Johan Doré Nellerod (2021) ,Master Thesis, Cyber Diplomacy at the United Nations: The Endeavours of the European Union and China to Determine 'Responsible State Behaviour in Cyberspace, Department of Political Science, University of Copenhagen