ISSN 2347-1522

■ Vol. V ■ Issue No. 5 September-October 2017

INDIA FOUNDATION JOURNAL

Opinions

- Global Health Diplomacy: A Strategic Opportunity for India
- India China Standoff: How and Why
- Three Warfares: A Prong of China's Military Strategy

Reports

- India-ASEAN Youth Summit-2017
- Eighth Round of India-Bangladesh Friendship Dialogue
- India Foundation Dialogue on The Future of India-UK Relations– British Elections, Brexit & Beyond
- Fudan-India Foundation 4th Annual Bilateral Dialogue at Shanghai
- Young Thinkers Meet 2017

Book Review

- Shivshankar Menon's "Choices: Inside the Making of India's Foreign Policy"

Focus: Cyber Security

- India's Cyber Security: Architecture and Imperatives - Davinder Kumar
- How is India Faring in the Cyber Domain - Cherian Samuel
- The Making of a Swadeshi Data Movement - Arun Mohan Sukumar
- International Cooperation on Cyber security - Asoke Kumar Mukerji
- Cyber Threats and Risk Mitigation - Subhash Katoch
- PLA in Electromagnetic Domain - P K Mallick

TABLE OF CONTENTS

India Foundation Journal

Vol. V
Issue No.5

September-October 2017

Editor
Maj Gen (Dr) Dhruv C Katoch

Assistant Editors
Srihari Avuthu
Shubhrastha

Publisher
India Foundation
New Delhi

E-mail
journal@indiafoundation.in

Website
www.indiafoundation.in

for private circulation only

Editor's Note

Dear Readers,

New technologies provide us with unimaginable possibilities in an increasingly interconnected world. They however, also create a new domain for conflict — Cyber conflict. Such conflict is likely to transcend the battlefield and pervade all civilian spaces as well, to include rail, road and air networks, water and electric supply systems, banking, stock exchange — indeed any activity that is dependent on computer based systems is vulnerable to cyber threats. Consequently, in recent years, threats originating in cyberspace have become an increasing cause of concern for countries across the globe. In many countries, such threats have been graded as the most pressing national security challenge. Today, these rapid technological developments have created a new domain of international politics, which mark the 'birth of cyberspace'.

Cyber warfare is thus a reality that we cannot ignore. Cyber-attacks on the battlefield will be aimed at key C4 nodes to disrupt battlefield network information systems. At the strategic level, attacks will focus on key financial and economic institutions, which could be devastating and may well force a country to compromise on core issues. Cyber warfare hence needs to be viewed holistically at the national level and both defensive and offensive measures must form part of this capability. We need to understand the role that both state and non state actors can play in the cyber domain and prepare accordingly. Under any circumstance, the influence of developments in the cyber domain must never be underestimated. The best talent available is in the youth of our country. They must be tapped into, to create cyber warfare units dealing with computer network attack, defence, and exploitation. We have no time to lose. Knowledge must remain our first line of defence.

India's Cyber Security: Architecture and Imperatives

Davinder Kumar*

Rapid and unprecedented growth of Information and Communication Technologies (ICT) and media with its speedy and all-pervasive penetration has ushered in the digital age. Not only has it brought the world together through globalisation, it has become the driver for economic growth. Technology and Information are the new normal of this digital transformation. This transition from an industrial to an information era has also ushered in a new security paradigm with new threats to both national and human security. With large scale automation, technology and connectivity, the developed nations are enjoying a much better quality of life. There exists a definite digital divide amongst the developed, developing and poor nations. This digital divide, coupled with the rising aspirations of the people accentuated by religious beliefs and cultural issues and technology denial have created serious security issues wherein new threats by way of cyber-crimes, cyber terrorism, cyber espionage and even cyber war have emerged making cyber security a strategic imperative at the national, regional and international levels.

Environmental Scan: India

While India has made considerable progress in the last decade or so towards the establishment of ICT infrastructure, enhancing the reach of the electronic media and extension of e-services in the finance, health and education sectors to ensure better governance, the development still remains differential. For example while India has the second largest number of Internet users in the world, it also has the second largest number of "Unconnected" population. The situation, however, is changing rapidly with the mobile telephone revolution which is under way and greater penetration of internet.

India's drive towards digital economy coupled with national projects like Digital India, Smart Cities, National Broadband Network and so on are altering the digital landscape rapidly with direct impact on governance, transparency and accountability. While there is a definite requirement of greater penetration of ICT for development and better governance, this rapid change towards a digital environment has brought to fore the challenges of cyber security. A cyber insecure Digital India Initiative can turn from a strategic asset to an unaffordable liability and a direct threat to national security. India, needs safe navigation through cyberspace for its prosperity, national and human security. Hence, ensuring complete cyber security of our assets and National Information Infrastructure is both a national strategic imperative and an urgent national mission.

Threat Landscape

From leaking debit card details to influencing the US Presidential Election, cyber-attacks have become a significant part of our political and social

*Lieutenant General Davinder Kumar is a former Signal Officer-in-Chief, Indian Army and former CEO & MD of Tata Advanced Systems.

discourse. Cyber threat exists 24/7 and manifests along the full spectrum starting from cybercrime to cyber espionage to cyber terrorism and cyber war.

Cyber crimes are a real threat today and are increasing very rapidly both in intensity and complexity with the spread of internet and smart phones. About eighty percent of cyber-attacks are related to cybercrimes. More importantly, cyber-crimes have changed the nature of conflict by blurring the line between state and non-state actors.

Cybercrimes are likely to increase exponentially with the fielding of virtual currency, Internet of Things, big data, cloud technology, drones, robotics, Blockchain and so on. Capabilities of hijacking a car, taking over the controls of an aircraft, cyber murder and remote injunction of viruses through drones and air crafts have already been demonstrated and in some cases, already inducted.

Dark net and Deep web are already being exploited for sale of vulnerabilities, weapons, recruitment of people in terrorist groups, drugs and so on.

Latest entrant to the long list of cyber-crimes is the installation of "Ransom Ware" to cripple a network or facility and demand ransom to restore the same. Recent ransomware attacks using Wanna Cry and Petya viruses have amply confirmed cyber as a "Weapon of Mass Disruption" with more than 300,000 computers affected across different sectors: health, finance, transport, ports and so on in 150 countries! Another major cyber-attack on HBO is still awaiting resolution with hackers demanding 2.5 million in Bit Coins.

One of the biggest cyber-attack in 2016 was the hacking of Indian debit cards wherein as many as 32 lakh debit cards belonging to various Indian banks were compromised resulting in the loss of Rs. 1.3 crore in fraudulent transactions as per National Payments Corporation of India (NPCI).

The Infamous hacker group "Legion Crew" made headlines in the sub-continent after hacking into the Twitter accounts and partial email dumps of prominent public figures such as politician Rahul Gandhi, businessman Vijay Mallya, and NDTV journalists Barkha Dutt and Ravish Kumar.

Cyber Espionage

Internet has become a very powerful source for intelligence collection in support of national, diplomatic, military, technology or economic objectives**.** It is estimated that more than 90 percent of "open source intelligence" is being obtained from the cyber world. It is economical and safe. Cyber espionage is also being used for technology theft and for launching probing missions on the critical infrastructure for possible exploitation later. The extent of threat can be gauged from the fact that Japan alone had 25.6 billion cyber-attacks in the year 2014 mostly for technology exfiltration. That is 900 cyber-attacks per second. The fact that attack Vectors for cyber espionage and cyber war are the same makes cyber espionage a major threat in being. Recent alleged interference by Russia in the democratic elections in France and the USA add another dimension to the threat landscape and the cyber intelligence.

Cyber Terrorism:

Coincidence between the physical and virtual worlds, as demonstrated by the STUXNET attack

on Iran's nuclear facility at Natanz in 2010, has put complete information infrastructure at risk. Targeted attacks on a nation's critical infrastructure like military installations, power plants, air traffic control, surface transport traffic control, telecommunication networks would be considered as part of cyber terrorism. These are low level, "short of war" attacks which would cripple part of a critical infrastructure or adversely affect the functioning of a business. These attacks are not large enough to warrant a military response but have the potential to inflict enough damage that numerous attacks over a long period of time could harm economy, complicating a policymaker's calculus for determining an appropriate response.

Social Media

Social Media like Face Book, Twitter, and LinkedIn has emerged as powerful tool for perception management, social engineering, cyber-crimes and intelligence. It has also emerged as a major instrument of waging "Asymmetric Warfare" through exploitation of the aspirations of people, differential development, varying religious beliefs and cultural leanings. These have also become attractive sources for recruitment and radicalisation by the terrorist organizations.

Nations across the world are putting legal frame work, infrastructure and human resource for monitoring this media to remain proactive. Major issue being privacy vs human/national security.

Cyber Warfare

It is universally acknowledged that the 21st century war will be highly "Cyber-centric" if not fully led by cyber theatre. Glimpses of these have been given by the Russian assault on Estonia and Ukraine. While in Estonia, it was pure cyber intervention, in Ukraine, it was a combination of cyber and Kinetic attacks wherein the bits preceded the bullets. This operation is a land mark in Cyber Enabled Warfare. Nations across the world have pronounced their doctrines of cyber warfare, have raised organisations to conduct cyber warfare and are busy in the making and testing of cyber weapons. USA is reported to have used "logic bombs" in Afghanistan and Syria to effectively neutralise their communication networks.

The Indian Scene

India is very vulnerable to cyber interventions due to certain strategic deficiencies, inadequate appreciation of the threat and rather tardy and disjointed implementation of policies. India was one of the handful of nations to promulgate Information Technology Act in year 2000 as a legal policy document to deal with cyber interventions. The same was revised in 2008. Similarly, the National Policy on Electronics was issued in 2012 and the National Cyber Security Policy in 2013. Yet, till a few years ago, well co-ordinated and focused efforts towards cyber security were missing except for the establishment of Computer Emergency Response Team – India (CERT-IN) and similar organisations at the state level and the Indian Army.

India's cyber security chief Gulshan Rai told Parliament's finance standing committee in July 2017, that cyber threats had evolved swiftly from viruses and "nuisance" attacks in the early 2000s to sophisticated malware and advanced denial of service, and could pose the risk of severely destructive attacks by 2020.

India will face increasingly sophisticated "destructive" cyber threats as compared to the "disruptive" attacks in the Indian cyberspace that are currently adding up to 200 million malware-related and 1,90,000 "unique" intrusions in any given week. The government — the Centre and states — is the main target of cyber-attacks, driven by motives ranging from theft, espionage and data extraction to counterfeiting. In 2015 and 2016, the government sector accounted for 27% and 29% of all cyber-attacks.

Other sectors high on the priority list of cyber criminals are banking, energy, telecom and defence, which along with the government, account for three-fourths of all cyber-attacks. The emergence of new services and apps, cloud and cognitive technologies, has made cyber security more challenging even as the value of data and its applications in commerce grows by the day, making cyber security a major task.

The incidence of e-transactions is rising with India logging in an estimated 2 billion such dealings a day as compared to around 54 billion worldwide, according to World Payments Report 2016.

Cyber-attacks use techniques and tools that help criminals evade detection with increasing refinement, and this has led the government to recognise cyber security as a "strategic domain" and devise strategies aimed at deepening cooperation at the international level. The PMO and the national security adviser are key elements overseeing a range of civilian and defence agencies with cyber security mandates.

Cyber Security Architecture

India is setting up its own 'cyber security architecture' that will comprise the National Cyber Coordination Centre (NCCC) for threat assessment and information sharing among stakeholders, the Cyber Operation Centre that will be jointly run by the NTRO and the armed forces for threat management and mitigation for identified critical sectors and defence, and the National Critical Information Infrastructure Protection Centre (NCIIPC) under the NTRO for providing cover to 'critical information infrastructure'.

Concurrently, the government is also coming up with a legal framework to deal with cyber security; has launched a drive for creating greater awareness to this threat and is creating necessary human resource with requisite skills. Major cyber security projects under implementation are given in the succeeding paragraphs.

National Cyber Coordination Centre (NCCC)

NCCC is a critical component of India's cyber security against hackers and espionage as well as track terrorist activity on line. A group of cyber security professionals and experts will look after the functioning of the Centre and track illegal and terror activities on line. It will run on similar lines as in the US, UK, France and Germany. Its mandate may also include cyber intelligence sharing.

Botnet Cleaning and Malware Analysis Centre

India has the largest number of Botnets in the world. To obviate and limit the threat due to botnets**,** the Government has recently set up a Botnet Cleaning and Malware Analysis Centre. The project is a part of Digital India programme

and aims to create safe and secure cyberspace. It will automatically detect botnets that trigger various cybercrimes and suggest the device owner to remove them from their device with their help.

Central Monitoring System (CMS)

Central Monitoring System, the Union Government's ambitious electronic intelligence monitoring system, is likely to start functioning fully by this year-end. According to the Ministry of Home Affairs officials, the hi-tech unit which will provide unhindered access to phone calls, text messages, and social media conversations to law enforcement agencies in real-time will have two units in the inaugural phase in Delhi and Bangalore.

National Critical Information Infrastructure Protection Centre (NCIIPC)

Article 70A (IT Act 2008) mandated the need for a special agency that would look at designated CIIs and evolve practices, policies and procedures to protect them from a cyber-attack. The National Critical Information Infrastructure Protection Centre (NCIIPC) was created and placed under the technical intelligence agency, the National Technical Research Organisation, to roll out counter-measures in cooperation with other security agencies and private corporate entities that man these critical sectors.

Protection of Power Sector

In December 2010, Ministry of Power had constituted CERTs (Computer Emergency Response Teams) for power sector i.e.; CERT-Thermal (nodal agency- National Thermal Power Corporation (NTPC)), CERT-Hydro (nodal agency- National Hydroelectric Power Corporation (NHPC)) and CERT-Transmission (nodal agency- Power Grid Corporation of India Limited (PGCIL)) to take necessary action to prevent cyber attacks in their domains. The State Power Utilities have also been advised to prepare their own sectorial Crisis Management Plan (CMP) and align themselves with the Nodal Agencies i.e. NTPC, NHPC & PGCIL and CERT - for the necessary actions.

Grid Security Expert System (GSES)

Grid Security Expert System (GSES) was developed by POWERGRID and it involves installation of knowledge based Supervisory Control and Data Acquisition (SCADA) system, numerical relays and Remote Terminal units up to 132 kV stations and the reliable Optical fibre Ground wire (OFGW) communication system. The objective of the GSES is implementation of the Automatic Defense mechanism to facilitate reliable and secure grid operation.

Crisis Management Plan

India has prepared a Crisis Management Plan (CMP) for countering cyber-attacks and cyber terrorism for preventing the large scale disruption in the functioning of critical information systems of Government, public and private sector resources and services. The Crisis Management Plan (CMP) for Countering Cyber Attacks and Cyber Terrorism outlines a framework for dealing with cyber related incidents for rapid identification, swift response and remedial actions to mitigate and recover from cyber related incidents impacting critical national processes.

Network Traffic Analysis System (NeTRA)

A monitoring and electronic surveillance project being executed by the DRDO**.** It appears to be Indian government's first attempt of mass surveillance rather than individual targets. It will scan the activities over the social networking websites like twitter and would scan the mails and chat transcript and even the voices in the internet traffic.

The above efforts are aligned towards developing a cyber defence capability. There is no information in the open domain regarding development of cyber offensive capabilities and their integration. Cyber space is essentially "Offence Dominant" by its very character and cyber power includes both defensive and offensive capabilities backed by appropriate organisation, technology, skilled human resource and a well-developed defence electronic manufacturing and components base.

Imperatives

India needs national scale effort supported by political will, adequate funding, contemporary technology and skilled people to realize necessary cyber security capability. These imperatives would require synergy amongst various ministries and agencies through appropriate policy framework and organisation and must be executed concurrently. Some of the essential imperatives are given in the succeeding paragraphs.

Establish National Cyber Security Commission (NCSC) – a fully empowered body with its own department, on the lines of Space Commission and Atomic Energy Commission. The country needs to build thought leadership and weave together India's potential in cyber security under one organisation. NCSC will have the onerous tasks of creating synergy amongst various stake holders through an enabling policy framework; developing technology, manpower, industry clusters, education standards and certification, intelligence and counter intelligence mechanisms, cyber forensics, security standards, and policy research. It will also coordinate with all ministries for National Critical Information Infrastructure (NCII) in their areas. It will play a catalytic role for the requirements of military in cyber warfare.

The National Cyber Security Policy 2013 needs to be revisited urgently in the light of rapid pace of technology development and very dynamic threat scenario**.** This policy should be translated to a time bound action plan in consonance with the national cyber security doctrine and specify clearly the responsibility for its execution and accountability. The policy, action plan, organisation and assured budgetary support must be discussed and approved by the Parliament.

Develop Cyber War Capability: India urgently needs to develop policies and capabilities in this 'Fifth' domain of war. These cannot wait and must be taken up on top most priority in a "Mission Mode" by the Services. The situation and threats to India are unique and hence there is the necessity of developing an indigenous solution in consonance with the doctrine to include organisation, technology, skill sets, training infrastructure and R&D. Immediate raising of an Indian Cyber Command is a national strategic imperative.

Energise "Make in India" Programme

India announced her National Electronic Policy (NEP) in 2012 with a view to establish an Electronic System Design and Manufacturing (ESDM) eco system and manufacture of semi-conductors in the country. Unfortunately, the scheme did not take off inspite of the fact that it offered attractive financial and taxation terms. This scheme has now been given a push under the "Make in India" programme. Absence of electronic manufacturing base and indigenous semi-conductor manufacturing capability in the country are strategic deficiencies. These are absolutely essential and fundamental pre-requisites for cyber security and need immediate attention at the highest level.

Cyber Policy Research Centre: There is no think tank that is studying policies and documents being produced by groupings of governments, industry, civil society, academia, interested organisations and international policy making organisations. Thousands of pages are being churned out, which require deeper understanding through analysis and discussions to decide on what is in India's interest. We are unable to address policy as well as operational issues due to the lack of focused studies. Numerous NGOs created at the behest of foreign governments, are obfuscating policy discussions to derail national positions. Also as technology evolves, a large amount of cyber security research and policies require timely revision.

Cyber Threat Intelligence Centre: India needs to have cyber analysis centers which collects attack data on various infrastructures, financial systems, web sites and services; correlate "big data" generated from government with financial and commercial data to create patterns and suggest anomalies, for advance preventive actions.

Cyber Workforce development: There is an urgent requirement to have a national plan to develop cyber security workforce and an associated cadre. NCSP 2013 has set up a target of five lakhs skilled cyber resource in the non-formal sector for cyber security and also to exploit the business opportunity of providing services to global customers by 2018. India also must lay emphasis on developing "Science of Cyber Security".

R&D for product development: India needs focused R&D in the development of safe products; discovery and analysis of vulnerabilities, fixing attribution and design of cyber weapons. Manufacturing and export of cyber security products presents a very attractive opportunity for India.

Security Standards and Frameworks, Audit: India needs to develop and promulgate the cyber security standards and frameworks for development, and audit processes for assurance of protection of our NCII. Enabling Policy measures are required to encourage establishment of testing labs for managing ICT Supply Chain Risks.

Cyber-crime investigations: There is an urgent need for development and continual upgradation of cyber forensics capabilities and investigating skills with our law enforcement agencies (LEAs), to handle cyber-crimes in the ever expanding proliferation of devices, platforms, big data, Internet of Things, mobility and social media.

Assurance Framework, Test & Certification: There is an immediate requirement of setting up a national cyber test facility providing for

network emulation, monitoring and audit, vulnerability analysis, simulated attacks, graduated response, performance analysis and security assurance modeling.

Build Thought Leadership, Executive/ Political Sponsors: Build cyber security savvy leadership, subject matter experts, solution architects and system engineers so as to address the inadequate comprehension of lack of cyber security capability and its bearing on national security including the military dimension.

Leveraging Diaspora: Indian diaspora is at the fore front of building security technologies, platforms and solutions across world class institutions and industry in USA and Europe. They can be the biggest catalyst in building cyber security capability. Proactive and aggressive steps should be taken to leverage the diaspora.

Outreach Programme to Attract Industry. Government needs to make it attractive for the private sector to invest in capability building through innovative mechanisms, such as funding development of new technologies, committing to buy from partner companies etc. Both the Government and the Industry must recognize multi-billion opportunity in cyber security related products and services and cash on this through a focused and proactive approach as was done for IT.

Establish Cyber Policy Research Centre: A Think-tank funded by the government/Industry, for studying all facets of cyberspace and making policy recommendations to the government.

In this digitally connected world, development of full spectrum cyber security along with an electronic industrial base, skilled human resource, enabling policy and legal frameworks, assured financial support, R&D and so on, in consonance with the national security and cyber doctrines, is a national imperative. The digital world of today demands "Technical Sovereignty" and complete protection of data to ensure national and human security. India must ensure these for continued development and securing her rightful place in the comity of nations.

◆◆◆

How is India Faring in the Cyber Domain

Cherian Samuel*

With Independence Day seeing a flurry of articles on India's progress over the years, now is as good a time as any to see how India has fared in the cyber domain. On the face of it, it would seem that India is no better or worse off than other countries. It has not faced any debilitating cyber attacks despite having adversarial relations with countries that have advanced cyber capabilities. Experts ascribe this to the fact that friend and foe alike are content to sit on the networks and harvest the data for information. However, successive stories of leakage of data are sufficient to indicate there are any number of vulnerabilities in networks, systems and software that can be exploited by adversaries. The increasing reported instances of cybercrime only serves to bear this out. On the policy front, while there has been considerable progress in fashioning proactive policies in a number of areas central to cyber security from safeguarding critical information infrastructure to fostering start-ups, the moot questions are whether a) these policies are sufficient and b) whether they are being effectively implemented. There are other areas where policies are urgently needed but are developing at a snail's pace such as in encryption, even as new technological developments such as blockchain technologies are in urgent need of policy direction to enable a healthy environment for their development. With the increasing militarisation of cyberspace, there is also a need for understanding the role of the military and the intelligence agencies in cyberspace, and developing doctrines as well as concretising operational issues such as chains of command, etc. While India has taken a more pro-active interest in the international debates on cyber security, and is actively participating in international fora, its position on many issues is yet to be clearly delineated. The deeply interlinked nature of activities in cyberspace means that all these policy issues and areas are deeply interlinked which creates enormous challenges for policy makers.

India had a head start in the cyber-domain, being one of the first countries to have an Information Technology Act, and to set up Computer Emergency Response Team (CERT). The potential for Information and Communications Technologies to drive growth and development was seen as early as the 1970s when the National Informatics Centre (NIC) was setup to provide information technology solutions to the government. The 1980s saw increased utilisation of communications technologies through the establishment of country-wide networks, among these, the National Informatics Centre Network (NICNET), a nationwide VSAT network for public sector organisations, which also connected the central government with the state governments and district administrations, and the Education and Research Network (ERNET), which served the academic and research communities. Internet service for the public was made available from

*Cherian Samuel is Research Fellow in the Strategic Technologies Centre at the Institute for Defence Studies and Analyses (IDSA). Views expressed are personal.

August 14, 1995. Today, India has not only the second largest user base worldwide with over 462 million users, but also has the fastest growth with an increase of 108 million over the previous year. This was largely due to the drop in data tariffs by over 75% over the previous year.

Successive governments have been proactive in using information and communication technologies (ICT) to improve governance and accelerate development. The present government has taken these efforts to a new level by making internet connectivity and digitalisation the cornerstone of many of its activities. Just one of these campaigns, the Digital India Campaign has a number of ambitious goals, from creating broadband highways, improving delivery of government services, and reducing electronics imports. Others like Start-up India endeavour to have digital products created in India rather than just consuming those created elsewhere. The Aadhaar unique identification card initiative, with over a billion numbers generated, functions on a digital backbone, with the biometric data stored in a central database.

The vast expansion in all things digital has increased the attack surface for adversaries. Recent attacks around the world on critical infrastructure ranging from electricity grids to financial institutions to even nuclear plants make the various doomsday scenarios of Cyber Armageddon, quite plausible. Response and remediation to these attacks show that governments, largely have a limited role in emergency response to such attacks, other than monitoring and providing advisories through the relevant organisations. Their role is more towards pre-empting attacks, through, on the one hand, enacting policies to reduce the risks and locate vulnerabilities, as well as formulating broader policies that enhance security but are also flexible enough to allow for openness, innovation and privacy. These policies need to be addressed across many domains, from law enforcement, to commerce, to data security, as well as India's approach to global internet governance policy.

How has India fared so far? In terms of creating legal and administrative frameworks, this has been an on-going process for over two decades though implementing them has proved to be the more difficult part. Though many of them are deeply interlinked and should by rights be carefully sequenced, these frameworks have often been developed piecemeal and in isolation, and have taken an inordinately long time to implement in a domain where policymaking cannot keep pace with technology even in the most advanced countries. To give a few examples, a privacy law and a data protection law are essential to safeguard the individual at a time when companies are mining data streams of individuals for a variety of purposes and even selling them to third parties. In terms of implementation, the most glaring example is that of the Cyber Appellate Tribunal the apex body to try cases of cyber fraud which has been without a Chairperson since 2011 and has nearly all the cases from 2010 in pending status. Cases of cybercrime have gone up exponentially even as the rate of conviction remain abysmally low. Companies and individuals are easily susceptible to cybercrime because of low cyber literacy, lack of awareness especially about cyber hygiene and best practices.

Policy makers, whether in the Ministry of

Home Affairs (looking at cybercrime), the Ministry of Electronics and Information Technology (looking at issues of cyber security) or at nodal agencies are hamstrung by a number of seemingly immutable factors, ranging from the fact that much of the software and hardware is of foreign origin, and much of the data resides on foreign servers. This is getting further exacerbated with increasing digitalisation as companies in just about every sector, critical or otherwise, are entering into collaboration with application service providers without undertaking due diligence, in a rush to provide apps and services to customers. The security ramifications of the headlong rush to digitalisation are yet to be fully comprehended. The fact that much of the infrastructure rests in the privates sector also hamstrings the government's room for manoeuvre in terms of fashioning and implementing policies to secure the digital environment. As a case in point, in just one sector, telecom, the National Telecom Policy of 2012 had set a target for domestic telecom equipment to meet Indian telecom sector demands to the extent of 60-80 per cent by 2020 after it was noted that over 60% of the equipment was being sourced from China. That laudable goal notwithstanding, the fact is that even today, the vast majority of telecom equipment, amounting to Rs. 70,000 crores annually, continues to be imported from China.

The sheer size of the population, the federal setup, legacy issues, the multiplicity of agencies concerned with cyber security, lack of experienced and expert manpower in not just core areas of cyber security, but also in law enforcement and the judiciary, are all factors that will see the cyberspace environment become progressively worse before it gets better. The security aspects of new technologies and concepts from cloud computing to the internet of things and driverless cars to crypto-currencies, to name just a few, will provide more regulatory and policy headaches for policymakers in the coming days.

The external environment has also turned darker in recent times, as countries turn to militarisation following the failure of collaborative efforts to evolve norms to secure cyberspace. Norms development has been an on-going process for well over a decade in the United Nations and other fora, and for a time, looked to be making some progress, particularly in the Group of Governmental experts process instituted by the First Committee of the United General Assembly tasked with promoting Peace and Disarmament. The very success of the process seems to have led to its own un-doing as different groups of countries tried to secure their interests by putting forward untenable proposals. While the United States and its allies were supportive of the process initially, the bias towards multi-lateralism is probably one reason why there was no attempt made at arriving at a consensus report leading to a collapse of the process in 2017.

India has participated in many of the norm-making mechanisms related to cyber-security though it has tended to take nuanced positions based on its interests. The preference has hitherto been for multilateral fora since India faces the same problems other developing countries face at multi-stakeholder fora; that of limited participation due to limited funding for other stakeholder, disinterest on the part of stakeholders in the private sector, as well as limited domain expertise and exposure.

Efforts are being made to enhance participation in multi-stakeholder fora, be it in internet governance or cyber security. Having said that, the multilateral/ multi-stakeholder debate has taken on the shape of a proxy battle on ideological lines. As security considerations come to the fore, even liberal Western countries are imposing stringent regulations and laws without consulting other stakeholders.

In fact, India's vision of a fair and equitable multi-stakeholder mechanism could be said to blur the distinction between multi-lateralism and multistakeholderism, viewing this as a false dichotomy. In his message to ICANN53 where India formally signed up to the multi-stakeholder process, the Minister of Communications mooted a 'multi-layered' system of multilateral and multi-stakeholder institutions working on a common platform that will support equity, innovation, collaboration and inclusion. India has begun to more actively participate in organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN), the *de facto* global internet governing body, and is also holding the next iteration of the Global Conference on Cyberspace under the aegis of the London Process, a state-sponsored summit originally initiated to propagate the values and ideals of a global and open cyberspace. On the whole though, as consensus on the basic tenets of securing cyberspace and the means of doing so continues to evade the global community, the various seminars, conferences and commissions risk being relegated to being nothing more than talking shops.

On the bilateral front, India has signed MoUs on enhancing cyber security co-operation with a number of countries. There has also been a deepening of dialogues with a few countries such as Israel, the United States and Russia with substantive proposals on exchange of information, expertise and co-operation in research and development. Co-operation with the United States is the most crucial but also the most problematic. On the law enforcement side, there are multiple hindrances when it comes to co-operation ranging from lack of familiarity with US procedures and laws, and using out-dated mechanisms such as mutual legal assistance treaties (MLATS) and Letters Rogatory to obtain information and evidence for judicial cases that take an inordinate amount of time and effort to process. On the intelligence side, historically, effective two-way co-operation has been less than optimal since the agencies in the US intelligence constellation tend to provide information on a need-to-know basis. The cyber intelligence agencies have gone a step further and have been found actively hacking into the networks of friends and foes alike.

The militarisation of cyberspace continues apace as countries set up cyber commands, and gather up cyber ammunition in the form of exploits, vulnerabilities and malware. The United States has, in recent days, elevated the status of its Cyber Command to that of a Combatant Command. Though this is largely an administrative decision to separate it from the National Security Agency (NSA), it further accentuates the emerging arms race in cyberspace. India's approach has been exceptional and sober, with the government taking a graduated response, first undertaking to set up a Cyber Defence Agency which would presumably upgraded to a Cyber Command. While this is a

measured and restrained approach, scaling up should be a continuous process with set timelines, fixed structures and budgets. While the services are currently struggling jointness in the Armed Forces, jointness in cyber security should go beyond the Armed Forces and merge civilian capabilities as well. While on the one hand, the Armed forces bring in the expertise, operational capability and a clear mandate to defend the nation from any external threat and also house technical expertise, the private sector also has much to contribute in terms of domain knowledge, technical and financial resources. A cyber strategy would be effective only if it succeeds in synchronising the capacities, infrastructure and expertise spread throughout the government, the armed forces and the private sector.

The fact that the country has not yet been subject to a cyber attack of a magnitude that would impact on the life of the citizens, or cause the economy to crash should not give rise to complacency and the feeling that "all is well" as far as the country's cyber security is concerned. Attacks in the recent past have taken place through known vulnerabilities, as in the case of the Wannacry ransomware attack, as well as through unknown vectors. While some progress has been made in setting in place structures to improve the country's cyber security posture such as appointing a National Cyber Security Co-ordinator, setting up a National Cyber Co-ordination Centre, creating sectoral CERTs, activating the National Cyber Infrastructure Protection Centre, augmenting the expertise of the judiciary and of law enforcement, providing funding for R&D, more remains to be done. At the operational level, the most pressing issues are providing existing agencies with more teeth to enforce regulatory requirements, whether it be in reporting cyber attacks or sharing information. The capacities and capabilities of these agencies should be augmented to the required level. This also holds true for law enforcement and forensic agencies as well. At the policy making level, the time has probably come to have cyber security elevated as a specific Ministerial level responsibility to send the message down the line of its importance. This is not to suggest that a separate Ministry with attendant bureaucracy be set up but that the subject itself should be elevated to the apex level. Ultimately, the conversation that needs to take place is that between strategic experts, domain experts and policy makers to pinpoint the specific areas of weakness and how they can be plugged, the strategic calculations behind attacks, the policy actions that need to be taken to secure the country's cyberspace, and that dialogue is, as yet, not happening to a sufficient degree.

◆◆◆

The Making of a *Swadeshi* Data Movement

Arun Mohan Sukumar*

Former chairman of the Unique Identification Authority of India (UIDAI) and architect of the Aadhaar initiative Nandan Nilekani recently made the case for a "data inversion" policy, requiring businesses operating in India to return the data they collect to the user.[1] Over several iterations of this proposal, Mr. Nilekani has argued data of Indians is at the risk of being "colonised" by big technology corporations, and data inversion can "empower" the user.[2] A strong data protection framework, he suggests, would give users the right to "pull out" their data anytime. "They can choose what they want to be part of, and what they don't."[3]

Nilekani's comments are significant because they come in the backdrop of efforts by him and other technology evangelists — both from government and the private sector — to make India a "data-rich" economy. At the launch of Reliance Industries Ltd's digital offering 'Jio' early this year, its chairman Mukesh Ambani declared "data is the new oil"[4], with immense potential to "bring benefit to the people". In the same vein, Information Technology minister Ravi Shankar Prasad characterised data-driven, "digital" governance as "honest" and "transparent".[5] In a country whose digital economy has been largely serviced by American and Chinese companies, the desire among policymakers and home-grown businesses to retain agency over the data produced by consumers is acute.

Nilekani's data inversion proposal is not an altogether radical concept. As the former Infosys CEO has himself acknowledged, there is comparable legislation in the United States.[6] The Dodd-Frank Wall Street Reform and Consumer Protection Act, for instance, requires financial and banking institutions to maintain data about lending practices to small businesses.[7] This information has to be made available to "any member of the public" upon requests made according to statutorily prescribed procedure. The provision, which has met with controversy,[8] is aimed at ensuring "fair lending" practices through closer scrutiny of potentially discriminatory terms of financing for small businesses. But it also provides fintech startups precisely the data that they need to build digital platforms that cater to local needs.

But were such a proposal to be implemented in India, would it really "empower" the user?

At the heart of the 'data inversion' proposal lies the expectation that users — made owners of their data — will subsequently hand it over to Indian start-ups. Indian companies today have neither the giant data sets nor the analytics capabilities needed to create technology-driven platforms in the same manner as an UBER or AirBnB, but the ready availability of user data may level the playing field. The "data inversion" proposal is driven by the same motivations as the Swadeshi movement of the early 20th century, which sought to revive the textiles industry in Bengal and other parts of India that had suffered on account of Britain's surging exports to its biggest colony and market. Then, cotton mills in Manchester and Lancashire had taken

*Arun Mohan Sukumar is Head, ORF Cyber Security and Internet Governance Initiative.

advantage of rising market demand in India, supplying products that were acknowledged to be imitations of Indian methods of dyeing and printing.[9] Unlike textiles however, data is a "non-rivalrous" resource. A *swadeshi* data movement would not involve any boycott of foreign digital services: to the contrary, companies based outside India too will benefit from gaining access to a larger pool of user data in the country.

Key to harvesting such data would be the ready availability of Application Programming Interfaces (APIs) upon which Indian companies can build their digital platforms. The current suite of APIs developed by the iSpirt foundation — collectively called India Stack — already hosts several tools that developers can integrate into their platforms. For instance, state and central government departments as well as major Indian businesses have already absorbed the "Aadhaar eKYC" API to digitally verify their consumers without seeking physical copies of identification documents. The eKYC API allows a business to build a software platform that taps into the Aadhaar database (with the user's consent) to extract authentic details about her date of birth, address of residence etc, in the process removing the need to reinvent the wheel and spend lakhs of rupees in building a customer database. Similarly, the Unified Payments Interface - another API developed by the volunteer-driven iSpirit — allows businesses to create digital markers beyond just banking address to effect instantaneous transfers of money. These markers may be Aadhaar numbers, specially created UPI addresses, or just phone numbers. That platforms developed in Silicon Valley, like WhatsApp and Uber, have begun to integrate UPI-driven payments in their products is an indications that APIs developed in India can offer competitive tools for global markets.[10]

If India Stack currently hosts "first-generation" APIs that run on the back of large, government databases like Aadhaar, its progression into a more diverse set of tools for businesses and public agencies will be driven by developers' access to richer data sets. The Aadhaar platform provides barebones information for personal identification, and it would neither be prudent — on account of security reasons — nor desirable to link it to other sensitive, tertiary information about a citizen such as her health records. The Indian government is the custodian of vast troves of data about its population, but until such time there is a cohesive effort to digitise this data and protect it with appropriate safeguards, software developers will have to rely on information provided by users on their existing apps. If the user were to be the "owner" of data provided to large technology companies based abroad, it is likely she will provide it to Indian app developers that can provide targeted, locally relevant services (weather patterns, *mandi* rates for perishable goods, public transportation timings etc). In some cases, the user may be legally required to provide this information in return for governance benefits.

This process of transmission of data — either *de novo* information or data that has been "returned" by other platforms — from the user to Indian digital platforms arguably marks the genesis of a *swadeshi* data movement. In some respects, this process has already begun with the widespread

adoption of Aadhaar-enabled platforms, which allow the user to authenticate her private transactions through data shared with the government.

The availability of data for Indian companies to innovate for local needs is of course a positive development, but in the absence of a clear data protection regime, the jury is still out on the role of the citizen in this movement. In other words: what determines the success of a home-grown data movement? Is it driven by the technological innovations and bottom-lines of Indian businesses? Is another key metric the ability of governments in India to provide digital governance services at affordable cost to citizens? Or is it also the ability of Indian users to retain agency over their data, and determine precisely what can be shared with companies and government agencies?

The Supreme Court of India in its landmark ruling on the 'right to privacy' in August 2017 directly addressed the question of the user's agency over her data. The verdict — which affirmed the existence of a fundamental right to privacy — acknowledged that the "state may have justifiable reasons for the storage and collection of data" but also held that Indian data laws should protect the "autonomy" of the individual or the user.[11] The Court cited with approval the "privacy principles" outlined by the 2012 report submitted to the Planning Commission by a Group of Experts led by Justice A.P. Shah. These principles underline statutory limitations on data collection and access by state and non-state actors to users' data, as well as the importance of consent in collecting and sharing data with third parties. Some of these principles have already been absorbed, albeit in a rudimentary form, in the data protection guidelines crafted under the Information Technology Act, 2008.

But for a *swadeshi* movement to make India a data-rich economy to succeed, the user should be more than just the passive recipient of e-governance services or innovative digital platforms. The Indian user should play a crucial and autonomous role in determining the kind of data that is shared with the government and the private sector. Often, individuals - especially first generation internet users - agree to share their data with apps and services without understanding or being informed about the exact purposes to which such data may be deployed. The Supreme Court's recent judgement has rightly acknowledged the "centrality" of user consent, but the Indian government should go beyond consent- or permissions-based approaches in its national data protection framework. Faced with better awareness of the nature and functions of digital platforms they interact with, Indian users can make informed choices about the data they share. This in turn would spur the creation of digital products and services that address a consumer-driven demand or need. It would avoid the problem of all-pervasive collection of data, which often results in unchecked or illegal surveillance, cyber security vulnerabilities and data leakages.

The autonomy of the Indian user in digital spaces should be protected by the state through a legal framework that addresses three distinct relationships: user-government, user-private sector, and government-private sector. Of these three interactions, Indian law — through policies such as *The Information Technology (Reasonable*

security practices and procedures and sensitive personal data or information) Rules, 2011 — currently accounts for the collection of data by mobile applications and services, but does so in very broad terms that essentially allow companies to gather and share information they determine to be relevant to their products' functionalities.[12] The user's consent, in such a scenario, is made perfunctory. A growing, global body of research suggests that the permissions-based model of data sharing with digital applications does little to illuminate users' understanding of privacy and indeed, the nature of the apps themselves.[13]

Regulators in other jurisdictions have challenged the concept of "binary, one-time" consent given that "unprecedented amounts of personal information are collected by, and shared among, a myriad of often invisible players who use it for a host of purposes, both existing and not yet conceived of."[14] The risk of users not sharing relevant information is also real, as research suggests many will simply reject requests to access data if they are unaware of the context in which personal information is share with an app.[15] The user-private sector engagement in India must take into account the unique requirements of the online population and address how the user can retain agency over the sharing and collection of her data based on the context.

Meanwhile, the relationship between the Indian government and the digital citizen is mediated by statutes like the UIDAI Act which place limits on the sharing of sensitive and biometric information. Nevertheless, this legal framework does not account for the linking of Aadhaar information to tertiary public and private databases that may be vulnerable to leaks or cyber attacks. There are also few statutory mechanisms that ensure the state's accountability on policies around Aadhaar linkages with other government welfare programs.

Finally, there are no regulatory mechanisms currently in place to evaluate data sharing between public agencies and businesses across digital platforms. The UIDAI Act admittedly includes penal provisions for the misuse of biometric information by the private sector, but as businesses tap into public databases to provide digital platforms that deal with healthcare, transportation and education, the automated sharing of such information must be carefully scrutinised for corporate misuse. Calls for an "open data" policy in India are not new, but they must be calibrated to ensure that the user is not marginalised in choices around collection and sharing of personal information.

A national data movement — one that encourages the free flow of information across public and private platforms, thereby providing opportunities for both to create innovative digital products — can only be sustained with the user at its centre. The user must not only be made aware of the information collected from devices and platforms, but also the implications of such data sharing for her privacy. A swadeshi movement must distinguish itself from the deterministic ethos of Silicon Valley, which seeks to design and impose technologies on communities for the ostensible purpose of solving their social and economic malaises. India's data revolution must instead be driven by contextual, local language platforms that respect both the needs and rights of the user.

References:

[1] *Nandan Nilekani, "Why India needs to be a data democracy", July 27, 2017, Livemint, http://www.livemint.com/Opinion/gm1MNTytiT3zRqxt1dXbhK/Why-India-needs-to-be-a-data-democracy.html*

[2] *"Need law where data collected is shared back with users: Nilekani", The Hindu Business Line, July 22, 2017, http://www.thehindubusinessline.com/info-tech/need-law-where-data-collected-is-shared-back-with-users-nilekani/article9784813.ece*

[3] Supra *n.1*

[4] *"Mukesh Ambani says data is new oil for fourth industrial revolution", The Economic Times, February 15, 2017* economictimes.indiatimes.com/articleshow/57173843.cms

[5] *"Digital India Summit 2017: 'Data is the new oil'; data important for new policy formulation, says Ravi Shankar Prasad", Financial Express, March 23, 2017* http://www.financialexpress.com/industry/digital-india-summit-2017-data-is-the-new-oil-data-important-for-new-policy-formulation-says-ravi-shankar-prasad/599220/

[6] *"Who Owns Personal Data: Technology and Policy Frameworks", Aug 17, 2017,* https://www.youtube.com/watch?v=mwC1kjaWV6g&feature=youtu.be&utm_content=buffer1798b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

[7] *Section 1071, "Small Business Data Collection",The Dodd–Frank Wall Street Reform and Consumer Protection* ***Act*** *(Pub.L. 111–203, H.R. 4173)* http://www.dodd-frank-act.us/Dodd_Frank_Act_Text_Section_1071.html

[8] *"The CFPB Wants Data On Small Business Loans. Bankers Are Outraged", Forbes, May 29, 2017,* https://www.forbes.com/sites/robbmandelbaum/2017/05/29/the-cfpb-wants-data-on-small-business-loans-bankers-are-outraged/2

[9] *Prasannan Parthasarathi, "The European Response to Indian Cottons"* http://www.lse.ac.uk/economicHistory/Research/GEHN/GEHNPDF/PUNEParthasarathi.pdf

[10] *Arun Mohan Sukumar, "WhatsApp's Integration of UPI-Based Payments Has Strategic Consequences for India's Digital Economy", August 9, 2017, The Wire, https://thewire.in/165881/whatsapp-upi-bhim-digital-economy/*

[11] Justice K.S. Puttaswamy (Retd.) & And v. Union of India & Ors., *Writ Petition (Civil) No. 494 of 2012, para.181*

[12] *Rule 3,* The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf*

[13] *Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner and Nigel Shadbolt,*

"Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps", http://people.csail.mit.edu/ilaria/papers/CHI2017.pdf

[14] *Office of the Privacy Commissioner of Canada , "Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act*", *May 2016*, https://www.priv.gc.ca/media/1806/consent_201605_e.pdf

[15] *Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov, "Android Permissions Remystified: A Field Study on Contextual Integrity", September 2015,* https://www.ftc.gov/system/files/documents/public_comments/2015/09/00013-97595.pdf

◆◆◆

Prospects for Effective International Cooperation on Cyber Security

Asoke Kumar Mukerji*

When the first building blocks of cyber space[1] emerged in the 1960s, the concept of effective international cooperation for cybers ecurity was not a priority. Today, an ever-expanding information-based global cyber domain, dominated by wireless and fixed broadband, smartphones, the mobile Internet, cloud computing, open data, big data and social media, and linked infrastructures for transmission of information and the creation of a digital economy, is characterized by its trans-national or international character. It is generally accepted that this domain is multi-stakeholder in nature, and that information and communication technologies (ICTs) play a key role in the transformation of cyber space.

The four broadly accepted stakeholders in global cyber space are governments, businesses, academia and civil society. In terms of approaches to cyber security, the emergence of a digital society, both nationally and globally, which is dependent on the security of cyber space for myriad aspects of human endeavor, has significantly broadened the focus of governments. Businesses, licensed to operate in cyber space by the governments of their jurisdiction, have reflected this evolution, taking the lead in providing the necessary technologies and innovations to implement cyber security policies. Academia, which often partners businesses in innovating and applying new cyber technologies, has always played a vital role in spreading greater awareness of cyber issues, including vulnerabilities impacting on the security of cyber space. Civil society has contributed vigorously to upholding fundamental human rights in cyber space, while attempting to cope with cyber vulnerabilities which have a direct impact on the sanctity of human lives regardless of national boundaries.

It has become apparent to all stakeholders that the increasing speed and expansion of cyber space also contain inbuilt weaknesses which can be exploited to jeopardize the security of cyber space, including its use for meeting the aspirations of humanity for a prosperous future, driven by easily accessible ICTs. This has pushed the issue of cyber security to the forefront, and highlighted the need to ensure effective international cooperation on cyber issues, through coherence and cooperation among cyber space stakeholders.

Background

The United Nations General Assembly (UNGA) had first discussed scientific and technological developments in ICTs in the context of international security in 1998. It adopted a resolution that year sponsored by Russia following this discussion, which emphasized that such

*Asoke Kumar Mukerji is a former diplomat. He was India's Permanent Representative to the United Nations in New York from 2013-2015. He supervised India's participation in United Nations Review of the Tunis Agenda in 2015. He has led Government of India's multi-agency delegations for International Cooperation on Cyber Issues with the United States, Russian Federation, United Kingdom, and Japan during 2011-2013.

developments could have both civilian and military applications, and that "progress in science and technology for civilian applications needed to be maintained and encouraged".[2] Subsequently, in December 2002, a UNGA resolution called for the creation of a "global culture of cyber security", highlighting 9 elements which could contribute to this objective. These elements included awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.[3]

The initiative of the UNGA was dovetailed subsequently into the launch of global discussions on the "world information society" by the United Nations, resulting in multilaterally agreed outcomes from the United Nations' World Summit on the Information Society (or WSIS) at Geneva (2002) and Tunis (2005), referred to commonly as the "Tunis Agenda".[4] The need for the Tunis Agenda to keep up with momentous changes in cyber space between 2005 to 2015 was underscored by the UNGA in its High Level Review of the Tunis Agenda in December 2015.[5] The Review acknowledged the role of multi-stakeholders in cyber space, and called upon them to proactively accelerate the use of ICTs as a "means of implementation" for the global sustainable development framework. This framework had been unanimously adopted by world leaders at the UN Summit held three months earlier, in September 2015, as Agenda 2030, with its core 17 Sustainable Development Goals (SDGs).[6]

International discussions on cyber issues among all stakeholders recognize the concept that "a chain is as strong as its weakest link". Whether these issues relate to cyber security, or cyber-crime, or providing equitable access to cyber space, or bridging the "digital divide" between and within countries, it is acknowledged that progress (or failure) to secure any one area of cyber space will impact on the entire cyber domain.

Role of governments

Against this backdrop, the role of governments in creating an effective framework for international cooperation on cyber security is critical, as public policy is the prerogative of governments. Apart from their sovereign functions in negotiating and adopting an international legal architecture to facilitate various aspects of such cooperation, governments are themselves also increasingly the largest stakeholders of cyber space in terms of the implementation of their security and development policies.

Governments adopted a resolution in the UNGA in December 2003 on "developments in the field of information and telecommunications in the context of international security". They upheld the need for the free flow of information while looking at concepts aimed at strengthening cyber security. The resolution asked the UN Secretary General to seek the assistance of a Group of Governmental Experts (GGE), appointed on the "basis of equitable geographical distribution and with the help of Member States in a position to render such assistance", to report on the way forward to the UNGA.[7] From 2005 onwards the UNGA stipulated only the geographical representation criteria for the UN Secretary General to follow while appointing experts to the GGE.[8]

This approach determined the way the GGE

has functioned in two significant ways. First, in the absence of any multilateral roster of "experts" provided by member states, the UN Secretary General has selected countries, and not individual experts, to compose the GGE. The selected countries have been free to designate their experts for the discussions of the group. While some governments have opted for continuity in selecting their experts while participating in the different editions of the GGE, others have opted for rotating their nominees, which has prevented the GGE from adopting a collegial approach to its work. Secondly, discussions in the GGE have been skewed towards a narrow perspective on international cooperation on cyber security, based on the mandate of the First Committee of the UNGA, which is to look at "disarmament, global challenges and threats to peace that affect the international community …and challenges to the international security regime".[9] In the process, the initial emphasis of the UNGA in December 1998[10] to give primacy to civilian, rather than military, applications of ICTs has dropped by the wayside.

What has been the outcome of the work of the GGE so far on establishing effective international cooperation on cyber security? GGEs have normally worked for a two-year period. There have been five editions of the GGE constituted by the UN Secretary General so far between 2004-2017, with selected participating member states fluctuating from 15 in its first three editions to 20 for the fourth GGE and 25 for the fifth GGE. India has participated in the first three and the fifth GGEs.[11] The UN Secretary General has consistently nominated the five permanent members of the UN Security Council (China, France, Russia, the United Kingdom and the United States) to all editions of the GGE, implicitly linking its work to the dynamics of these five countries in the Security Council.

The first GGE could not agree on an agreed report in 2005, due to three areas of divergence. First, there was divergence on the impact of ICTs on national security and military affairs. Second, there were divergences on whether the proposed international framework for cyber security should focus only on the content, or only on the infrastructure, of ICTs. (Significantly, this divergence between content and infrastructure also led to the deadlock in updating the regulations of the specialized UN agency responsible for telecommunications, the International Telecommunications Union (ITU), at its Conference held in Dubai in 2012).[12] A third area of divergence was on the issue of technology transfer to developing countries. These divergences led the UNGA to ask the UN Secretary General to constitute another GGE in 2009.

The second GGE, constituted in 2009, issued a consensus report in 2010. It recommended dialogue among member states to reduce the risk and protect critical national and international cyber infrastructure; confidence building and risk-reduction measures, including the use of ICTs during conflict; capacity building; and elaboration of common terms and definitions in cyber security.

The third GGE in June 2013 agreed with the proposition that international law, and especially the UN Charter, applied to cyber space, while confirming that state sovereignty applied in cyber space. It underlined that cyber security should be in consonance with respect for human rights and

fundamental freedoms. It called on member states to respect their obligations not to allow proxies or non-state actors to use their jurisdictions for violating cyber security.

The fourth GGE in 2015 recommended some norms to secure cyber space. These included the recommendation that "States cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT." It emphasized that "States should guarantee full respect for human rights, including privacy and freedom of expression. A State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorized emergency response teams of another State or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions."[13]

Further progress was halted when the fifth GGE process reached a deadlock at its final meeting in June 2017. This was due to divergences on how international law would apply to the use of ICTs by states. In a public statement, the United States affirmed that "the framework of international law provides States with binding standards of behavior that can help reduce the risk of conflict by creating stable expectations of how States may and may not respond to cyber incidents they face", a view which was not agreed to by some other members of the GGE.[14]

Role of Businesses

While the GGE has articulated behavioral norms based on international law for international cooperation on cyber security, some trans-national businesses headquartered in the United States have taken initiatives to foster international cooperation based on the technology that drives cyber space. In February 2017, Microsoft advocated a "Digital Geneva Convention", that is meant to "commit governments to protecting civilians from nation-state attacks in times of peace" with the active assistance of technology companies.[15] Facebook, Microsoft, YouTube and Twitter joined hands in June 2017 to launch a Global Internet Forum to Counter Terrorism.[16]

Earlier, in June 2016, Microsoft had proposed a roadmap for developing offensive norms, defensive norms and industry norms. It pointed to the difficulty in attributing and countering threats to cyber-security because of "global connectivity, anonymity, and lack of traceability". Microsoft suggested that governments should adopt the model of public-private partnership in developing cyber security norms, as had been done in the case of the Financial Action Task Force (FATF), where consultation with the private sector helped effective implementation of financial norms, as well as a platform for private sector priorities to be addressed by governments.[17]

International cooperation on cyber security has also been pursued by businesses which maintain the global cyber infrastructure. Currently, 13 "root servers", administered by 12 entities, control the

functioning of global cyber space.[18] In this context, norms developed through platforms such as the Internet Corporation for Assigned Names and Numbers (or ICANN), have become relevant. The main functions of the ICANN are to allocate domain names, numbering resources, and decisions on internet protocol parameters. Each of these functions has a significant ground-level impact on international cooperation on cyber security. A similar ongoing role is being played by the professionals who create cyber space, represented by the Internet Engineering Task Force (IETF)[19].

Role of Academia

Academia's contribution to establishing an international framework of cooperation on cyber security has a long history. Its focus on people as well as technology enables academia to address one of the major challenges of cyber security, which is the human factor. Generating awareness is perhaps the most significant contribution that academia can make to effective international cooperation on cyber security, by preventing the exploitation of vulnerabilities in cyber space. The constant flow of graduates from academia into both governments and businesses represents a continuous upgradation to the international community's efforts to tackle issues of cyber security.

Academia has often taken the lead to make significant conceptual contributions to evolving an international framework of cooperation on cyber security. For example, almost a decade ago, a white paper prepared for the White House by Pradeep Khosla, the founding director of Carnegie Mellon's CyLab, advocated that a more relevant approach to cyber security policy would be to look at a "data-centric" rather than a "device-centric" approach.[20]

Apart from generating greater awareness of the vulnerabilities of cyber space, and looking at the issue of cyber security from a multidisciplinary perspective, academia also plays a hands-on role in ground-level international cyber security cooperation. This is well illustrated by two universities in the United States (University of Southern California and University of Maryland) who manage two of the 13 root servers of the internet. A focused participation in the global discussion on the need for international cooperation on cyber security is the hallmark of academic think-tanks across the world, though many of them are funded by sources looking at cyber security issues from a military perspective.

Role of Civil Society

Civil society is perhaps the most vocal stakeholder of cyber space, using cyber tools such as social media to advocate its views. Ensuring the upholding of fundamental human rights online has been recognized as one of the core advocacies of civil society as governments work to establish a framework for effective international cooperation on cyber security. These rights include, inter alia, freedom of expression, privacy, and human dignity.

The Way Ahead

As this brief review outlines, the current multilateral effort to create an international framework for effective international cooperation on cyber security through the GGE of the UNGA has probably reached its limit. Countries which are active in cyber space have initiated steps to position

their views on issues like cyber norms and application of international law in a confrontationist, rather than cooperative, mode. Without a cooperative approach among governments at the multilateral level, the initiatives taken by businesses, academia and civil society to augment an appropriate international framework are greatly diminished.

While bilateral and regional frameworks have been welcomed by the multilateral process under the United Nations, including during the Review of the Tunis Agenda in December 2015, the impact of these frameworks would be limited to participating countries. For effective global cyber security cooperation, the core focus must remain on a universally applicable framework, which has its focus on the weakest link in the global cyber chain.

How can this happen? The time has come for the UNGA to adopt a resolution to launch broad-based multilateral negotiations, with inputs from the major stakeholders, on international cooperation on cyber security. These negotiations should be launched by the UNGA as part of its review of the implementation of Agenda 2030.

The UNGA has acquired relevant experience for such multi-stakeholder negotiations, which have been led by governments, during the past few years, when global issues such as sustainable development and the evolution of a world information society were placed on the UNGA's agenda, and successful outcomes reached.

In any such future negotiations, some potential areas of divergence could arise. One issue would be who would decide on the question of attribution for attacks on cyber security, given the skepticism among a majority of UN member states for such issues to be referred to the UN Security Council as currently structured, where necessary structural reforms, including on decision-making, have been resisted by some of its permanent members. Another potential area of divergence would be in adopting a common template to counter perceived cyber security vulnerabilities in industrialized and developing countries, and where national capacities to respond to threats require technology transfers and financial flows. Divergent economic interests of major multinational ICT businesses and new emerging ICT businesses will inevitably be reflected in these negotiations when counter-measures are conceptualized. Negotiators will have to identify provisions drawn from applicable international law, including the UN Charter, the WTO's corpus of international trade law and international humanitarian law.

However, potential divergences cannot detract from the urgent need to secure global cyber space, through an internationally agreed framework on effective cooperation on cyber security. As the UNGA has pointed out repeatedly, the impact of effective international cooperation on cyber security is not only restricted to international peace and security, but also to development. In this context, there is need to broaden the negotiating mandate for an international framework to include the "development dimension" of cyber security, drawing upon the specific provisions contained in Agenda 2030 and the Tunis Agenda.

In any such international negotiation, the role of India in focusing on the "development dimension" of international cyber security cooperation will be crucial. The scale of India's national programmes which apply ICT for

development is unique, symbolized by the nine pillars of Digital India with its Aadhar database, provide a ground-level drawing board for conceptualizing and testing cyber security concepts, as well as the effectiveness of international cooperation in securing developmental programmes.[21] A special focus would need to be provided by India during these negotiations on the impact on designated critical national infrastructure sectors.[22] India's advocacy of using a "development" perspective in the process to create a supportive international framework for cooperation in cyber security will be relevant for a large number of other developing countries, who are prioritizing the use of ICTs to meet their sustainable development goals under Agenda 2030.

The objective should be the creation of a framework on cyber security which will serve the global cyber domain in the same manner that the United Nations Convention on the Law of the Seas (UNCLOS), which was negotiated between 1973 and 1982, serves the global maritime domain.

References:

[1] *Internet Society, "Brief History of the Internet". Available at http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet*

[2] *United Nations General Assembly Resolution A/RES/53/70 dated 4 December 1998. Available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement*

[3] *United Nations General Assembly Resolution A/RES/57/239 dated 20 December 2002. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239*

[4] *"Tunis Agenda for the Information Society". Available at http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html*

[5] *United Nations, "Outcome Document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society", UNGA Resolution A/RES/70/125 dated 1 February 2016. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/125*

[6] *United Nations, "Transforming our world: the 2030 Agenda for Sustainable Development". Available at https://sustainabledevelopment.un.org/post2015/transformingourworld*

[7] *United Nations General Assembly Resolution A/RES/58/32 of 8 December 2003. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/32*

[8] *United Nations General Assembly Resolution A/RES/60/45 dated 8 December 2005. Available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/45*

[9] *United Nations. "Disarmament and International Security: First Committee". Available at http://www.un.org/en/ga/first/*

[10] *See footnote 3 above.*

[11] *For a summary record of the work done by the four GGEs, the United Nations Office of Disarmament Affairs Fact Sheet, available at https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf is useful. India was omitted by the UN Secretary General for the Fourth GGE due to alleged pressures from other countries to apply the criteria for rotational representation. From the Asia-Pacific region, China, Japan, Malaysia and Pakistan were chosen by the UN Secretary General. India was re-nominated to the Fifth GGE by the Secretary General in 2016.*

[12] *For an outsider's account of this deadlock, see "What really happened in Dubai", Internet Governance Project, Georgia Tech. Available at*

http://www.internetgovernance.org/2012/12/13/what-really-happened-in-dubai/

[13] *United Nations. Report of the GGE to the UN Secretary General No. A/70/174 dated 22 July 2015. Available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement*

[14] *United States Department of State. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security ". Available at https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm*

[15] *"The need for a Digital Geneva Convention", Microsoft. Available at*

https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/

[16] *Global Internet Forum to Counter Terrorism. Available at*

https://blog.twitter.com/official/en_us/topics/company/2017/Global-Internet-Forum-to-Counter-Terrorism.html

[17] *"From Articulation to Implementation: Enabling progress on cyber-security norms", Microsoft. Available at*

https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cyber security-Norms_vFinal.pdf

[18] *A map of the 13 global root servers is available at http://www.root-servers.org*

For technical details on root servers and related issues, see "What are Root Name Servers", Netnod, Sweden. Available at https://www.netnod.se/i-root/what-are-root-name-servers

[19] *See "About the IETF". Available at https://www.ietf.org/about/*

[20] *EDUCAUSE Review. Academia's role in security cyberspace, Jared Cohon, 2009. Available at*

https://er.educause.edu/articles/2009/9/academias-role-in-securing-cyberspace

[21] *The breadth and depth of India's cyber profile was presented during the Review of the Tunis Agenda by the UNGA in December 2015. It is available at*

http://workspace.unpan.org/sites/Internet/Documents/UNPAN95026.pdf

[22] *For a discussion on the issues involved in protecting India's Critical National Infrastructure, see "Protection of Critical Information Infrastructure: an Indian Perspective" by Col. R.K. Sharma, The Digital Policy Portal, Observer Research Foundation. Available at*

http://www.digitalpolicy.org/protection-of-critical-information-infrastructure-an-indian-perspective/

◆◆◆

Cyber Threats and Risk Mitigation

Subhash Katoch*

"The single biggest existential threat that's out there, I think, is cyber."

Michael Mullen

Introduction

Digital is the new paradigm. All facets of life today are being disrupted by digital technology, changing the way things were done or are being done. This disruption is all around us, in day to day life as well as complex organisations like business, industry or military. The two technologies i.e. Information Technology and Communication Technology have ushered in new efficiencies, new ways to do things and this change is continuous and exponential. In the Indian context, the 'Digital India' thrust of the Government has taken our country in a new direction at a previously unimagined pace. IRCTC, Cashless transactions, E Governance, GSTN, E Banking, Bharat Net have all provided the means and reach to citizens and the Government to take up the task of development of our society, in an inclusive manner at a fast pace.

2. INTERNET and associated technologies have made it possible to disseminate information at the blink of the eye, re-engineer and control various processes, in every possible field. The society today has become heavily dependent on this digital infrastructure, the Cyber Space. It is the lifeline of economy and other structures of the society. If disrupted, the resultant mayhem would be catastrophic. Just imagine the chaos if the complete banking or transport or communication network is brought down, deliberately or due to a failure. All network and information infrastructure is planned with due backups catering for routine failure. However, there is a need to cater for disturbance caused by deliberate action.

3. Exploitation of cyberspace for degrading the digital civil and military infrastructure, poses a rapidly growing threat to national security of the country. Hence it's necessary to analyse the trends in cyber threats, assess how these can impact the environment in Indian scenario and how to mitigate this threat. As per CERT India, one cyber attack was reported every 10 minutes in the first six months of 2017. As many as 27,482 cases were reported from January to June, higher than 2016 when it was one in every 12 minutes.

Cyber Threats to Society

4. Criminals have used the Internet to sell drugs, guns, ammunition, forgeries (passports, driving licences) and financial information (credit card information, bank account login details). Online marketplace 'Silk Road' set up in 2011 by Ross Ulbrickt aka 'Dead Pirate Roberts', did business worth $1.2 billion (in Bitcoins), had

*Brig Subhash Katoch (Retd) is a highly technical professional with 37 years of comprehensive experience in military telecommunication technologies, data networks, cyber security, analytics, decision support systems, automation, database management, EMI/EMC testing and compliance. He holds a MBA from FMS, Delhi University, 2001; M.Phil. (Defence & Management), DAVV Indore, 2005; M.Sc. (Defence & Strategic Studies) Madras University, Chennai, 1993; M.Tech. (Computer science and Technology), IIT, Chennai, 1990.)

957,909 registered users before it was shut down in 2013. Site anonymity was maintained by using TOR (The Onion Router) and using bitcoins (a digital currency) for transactions. Silk Road provided a platform for trading in :

- Narcotics and controlled substances.
- Malicious software.
- Unlawful services such as hacking into Facebook, Twitter, Emails, Tutorials for hacking ATMs, Contacts for guns, arms, fake currency.
- Pirated content, digital goods.
- Forged Documents.

5. Another example was 'Dark Market' which facilitated buying and selling of stolen financial information. Set up in 2008 by Renukanth Subramanium in London, it had 2500 members dealing in stolen credit card data, login credentials and equipment for financial crimes. It was taken down in 2010. These organisations were fully organised with corporate like structure having administrators, moderators, Receivers, Hackers/ data thieves and users.

6. The two examples cited are living proof of availability of Cyber Crime as a Service (CCAAS) where sites or vendors are offering to buy - sell - hire - outsource all the sophisticated technologies of cyber threats. On the offer are:

- Specific hacker software.
- Secure Hosting.
- DDoS botnets.
- List of targets for Phishing schemes.
- Access to Critical Systems.
- Custom Virus development.
- Batches of credit card numbers.
- Zero day exploit exchanges. Cases where Administrators have zero day to fix the flaw, hence hackers have the maximum advantage.

7. Almost every part of daily life is becoming vulnerable as the dependence on digital technologies increases. Modern automobiles are totally driven by software, adopting the technology of 'drive by wire' wherein almost all functions are controlled by software. Many sensors and communications systems are integrated to make cars smart and the vehicle system can be configured and optimised using smart phones or laptops, making them vulnerable to hacking. Automotive cyber security researchers Charlie Miller and Chris Valasek hacked a 2014 Jeep Cherokee in 2015, using the radio used in entertainment system. In May 2017, FBI arrested members of a motorcycle gang accused to have hacked and stolen over 150 Jeep Wranglers from Southern California since 2014.

8. Attack on airline ground computer systems used for issuing flight plans can cause mayhem in the operations of airlines. Hacking of an airplane is possible by getting access to its satellite communication system through passenger WiFi and inflight infotainment system. There have been reported incidents of hacking of a plane in flight, causing it to climb by 'overwriting' code on thrust management computer. A cyber security consultant Chris Roberts told the FBI in May 2015 that he hacked into computer systems aboard airliners about 20 times and managed to control an aircraft engine during a flight.

9. The domain of Healthcare is also going through digital disruption. The diagnostics, sensors monitoring vital parameters, electronic medical

records (EMR), telemedicine, all these systems are vulnerable to cyber threats. Some possibilities are:

- Remote manipulation of drug infusion pumps.
- Altering digital medical records.
- Restart/reboot critical equipment.
- Spoof blood tests / other diagnostics.
- Changing temperature settings in systems storing blood or drugs.
- Bluetooth enabled defibrillators or pacemakers could be made to deliver random shocks to a patient's heart.

10. It is hard today to imagine life without WhatsApp, Google, Facebook, Amazon, Ola, Paytm, Netflix, et al. What most of us do not realise is that these services collect huge amount of data about users allowing them to understand each customer to improve their services and of course profits. This data of millions of Indians could be made available to enemy intelligence agencies who could find negative information about, say a policy maker and make her change a key decision. The location or movement of troops can be detected just based on location data change of service personnel. The possibilities of misuse of such data are endless.

11. The society is also facing the problem of addiction of younger generation to digital world and social media. Millennials or The Generation Y have grown up with these technologies and are vulnerable to exploitation by cyber criminals. 'Blue Whale Game' or 'The Game of death' claimed its first victim in India on 01 Aug 2017. The maker of the game Philipp Budeikin was convicted and sentenced to three years in jail in Russia. Using the 'Dark web', Budeikin played with the minds of impressionable young men and women inciting them to commit suicide. Child pornography, human trafficking, illegal money laundering and many more heinous crimes have been abetted through cyber technology.

12. Hackers are constantly looking for new ways to access data. Most recently, the way was as simple as a fish tank. The hackers attempted to acquire data from a North American casino by using an Internet-connected fish tank, according to a report released on 19 July 2017 by cyber security firm Darktrace. The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank. "Somebody got into the fish tank and used it to move around into other areas (of the network) and sent out data." The report said 10 GB of data were sent out to a device in Finland. As more products with the ability to connect to the Internet become available (IoT - Internet of Things), opportunities for hackers to access data through outside-the-box ways have risen. Recently FBI warned parents about the privacy risks of toys connected to the Internet, which could help a hacker learn a child's name, location and other personal information.

Cyber Threats in Military domain

13. Warfare has also been disrupted by this digital assault of technology. Technology has always been driven by the military and today all weapon systems and mechanics of warfare rely heavily on digital systems. Direct traditional warfare is changing into asymmetric warfare against traditional and non traditional enemies,

where cyber space provides a very potent arena with its tremendous and quick reach. Shaping perceptions, disseminating information across borders at a lightening pace, technology is making it difficult to anticipate the character of future conflict. Technology is providing means which can offset conventional capability and bring victory without bloodshed.

14. The increased dependency on communication and data networks, storage of information in cyber domain and its vulnerabilities, lack of mutual consent between countries on effective control of operations in cyber domain has brought in a new type of threat - Cyber warfare. Many countries and non state actors are conducting Cyber Espionage, Cyber Reconnaissance and are also involved in creating offensive Cyber Warfare capabilities. Cyber attacks and network intrusions, linked to nation states are being reported at an increased frequency. Major resources are being utilised on how to conduct Cyber Warfare rather than preventing it. There is lack of International dialogue and activity with respect to controlling cyberspace.

15. Exploitation of cyberspace for carrying out attacks on military infrastructure, government and financial institutions poses a rapidly growing threat to national security. Such attacks would more often than not be launched in peacetime by state or non state actors. Rather today, one must assume that most nations would be engaging in this form of warfare, all the time, as it has the advantage of :

- Attribution is difficult and attacker can choose timing, location and impact.
- Asymmetric tool ideal for nations with comparatively weaker conventional force to gain military advantage.
- Low cost and high impact option.
- Ideal option for non state actors.

16. All the major weapon systems are increasingly becoming digital as technology enables integration with sophisticated sensors, command and control systems for increased situational awareness, accuracy and lethality. Requirement of quick response, shortening of OODA loop requires automation and computer control of weapon systems. The increased dependence on digital technology brings in the element of cyber threats. The complex weapon systems with numerous components developed by different agencies, some using COTS technology, with millions of lines of code, are vulnerable to exploitation. Hidden bugs, trapdoors in software or hardware which could be triggered during war or at a chosen instant, cannot be ruled out.

17. Operation Orchard or 'The Silent Strike' was an Israeli airstrike on a suspected nuclear reactor in the Deir ez-Zor region of Syria, which occurred just after midnight on September 6, 2007. The attack denied by Israel, showcased its cyber warfare capabilities as Israeli electronic warfare (EW) systems took over Syria's air defence systems, feeding them a false sky-picture for the entire period of time that the Israeli fighter jets needed to cross into Syria, bomb the target and return. The compromising of the air defence system could only have been possible if a cyber attack induced a false sky picture. It is also believed that Mossad hacked into the computer of a senior Syrian government official in 2005-6 and planted a Trojan horse which siphoned off files containing detailed plans, photos of the illicit nuclear facility.

Risk Mitigation

18. The threat of cyber attacks will always exist in both civil and military domains which imposes a grave risk. Systems and ideas have to be evolved to mitigate this risk. Vulnerability is a measure of ability to prevent a security incident. The current security system and procedures represent the active steps one has taken to reduce the vulnerability. Vulnerability is a dynamic concept. It changes whenever the environment, operations, personnel, business and/or systems change. Each time a substantive security-related change occurs in an area, one needs to reconsider the vulnerability in that area. Hence continuous risk assessment would be needed in this domain.

19. Recognition of these threats and getting used to the idea that vulnerabilities exist is the first step. Most of us treat these scenarios as imaginary, something that happens to others. All victims of ransomeware like 'Wanna Cry' or 'Petya' realised the gravity of such an attack only after experiencing it. Most victims are not sure of unlocking their computers even if they pay the ransom. Essential components of defence such as Firewalls, Intrusion detection/prevention systems, Unified Threat Management systems, Encryption, Patch/ Password management and Antivirus systems must be used. Maintaining air gap between Internet and internal networks, use of wired media and secure storage reduce the vulnerability to a great extent.

20. Hackers are trying so many ingenious ways to break into systems, that the government will have to get involved in regulating digital systems. The expected onslaught of Internet of Things (IoT) products in near future makes it imperative. Getting everything to go through Government approval, on the cyber front, will raise questions about privacy and bureaucratic control but it may be the bare minimum required to protect the users. How to do this globally - would be a real challenge. As for what people can do to protect themselves against these kinds of attacks, education and awareness would be the start point. Consumers will have to educate themselves about digital products and take advantage of offered protection features. Latest operating systems and software must be used and continuously updated.

21. Data being collected by various companies and organisations need to be regulated. Data protection laws are not enough. The issue of where data is resident needs attention. Data is protected under the laws of the land where it is stored. Most of the social media and e-commerce companies store this data in US where No protection is afforded to data of non US citizens. Private information of Indians must be stored in India. Currently Indian government agencies are at the mercy of foreign agencies to get the data of own citizens which is totally unacceptable from a security perspective. The access to such data must be governed by Indian laws. The next war may not be physical but in the Cyber space and Data will be a key weapon. A country needs to protect its resources and should not be at the mercy of foreign governments and companies.

22. The Armed forces face the following challenges:

- Induction of systems in a quick time frame to make up shortages without proper risk

analysis will lead to disaster. Proper analysis, appropriate GSQR and testing is necessary to mitigate these risks.

- Ensure proper testing of all systems being inducted. Since the defence forces import most of the weapon systems currently, some components of these systems could have a trojan implanted which could be triggered when required. Proper EMI/EMC testing would mitigate a large component of this risk and prevent a 'Silent Strike'.
- Need to evolve effective response mechanism at organisational level to respond to day to day cyber attacks.
- Requirement of forming a cyber work force with requisite qualifications to handle emergent cyber threats.
- Synergy of effort at organisational level to develop best practices to handle cyber incidents.
- Plan and exercise Cyber Crisis Management at National and Defence Forces Level.

23. Some recommendations :

- Formulation of a National Cyber Security Policy. The release of the National Cyber Security Policy 2013 is an important step towards securing the Cyber space. The implementation of policies must be carried out in a time bound manner.
- Common communication infrastructure and agencies like 'National Cyber Coordination Centre' be established at national level for sharing and processing of information related to cyber threats.
- Define strategy at national level for conduct of cyber offensive activities and develop such capabilities.
- Proper laboratories with suitably trained manpower to conduct tests to check vulnerabilities, to keep pace with rapid technological changes and quickly support operational cyber-warriors with the latest upgrades, techniques and threats.
- Allocation of budget to enhance existing cyber capabilities both in defensive and offensive fields.

Conclusion

24. Cyberspace is increasingly becoming a place of risk and danger, vulnerable to hacks and threats. With today's civilisation dependent on interconnected cyber systems to virtually operate most of the critical systems that make our daily lives easier, it is obvious that cyber warfare will be the choice for many governments and non state actors in future conflicts, especially those with limited access to expensive, conventional weapons of mass destruction. Hence it is imperative that this field be given due importance and both offensive and defensive capabilities acquired in a time bound manner.

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace." – Newton Lee

◆◆◆

PLA in Electromagnetic Domain

P K Mallick*

Introduction

The PLA expects to fight intense short wars that will be very decisive. The ability of military forces to communicate and coordinate rapidly through Command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks means that military forces in Local Wars at the operational level will be agile, capable of high-tempo deep operations, resource-intensive, critically dependent on information and present in all warfare domains. China's military modernisation is underway, with the new PLA organisations aiming to establish a national and a theatre-level HQ for ground forces, turning the Second Artillery department into a full-fledged service, and creating a Strategic Support Force to manage the information domain including space, cyber and electronic warfare activities. This process started in 2015 and will end only in 2020 or later. The Central Military Commission (CMC) has been restructured in 15 departments and commission, the seven military regions have been reorganised into five geographical-operational theatre commands and each branch of the Army has been reorganised as a service HQ for the forces, to separate the administrative services from the operational dynamics. The reforms also aim to reduce manpower in the Chinese military.

PLA Theory on Modern Warfare

The PLA envisions future conflicts under the conceptual umbrella of Integrated Network Electronic Warfare or INEW. It combines coordinated use of computer network operations (CNOs), electronic warfare (EW) and kinetic strikes designed to paralyse an enemy's networked information systems, by creating "blind spots" against an adversary's C4ISR systems. The PLA's C4ISR programmes support the ground forces, navy, air force, missile forces, nuclear doctrine, and space warfare. Its operational concepts for employing traditional signals intelligence and electronic warfare have expanded to include cyber warfare; kinetic and cyber attacks on satellites; and information confrontation operations across the electromagnetic spectrum. The PLA, under the "Integrated Network Electronic Warfare" doctrine, has been paying significant attention to information warfare in the past 10-15 years, not only looking at Cyber Warfare, but also battlefield Electronic Warfare (EW).

Chinese EW doctrine emphasises using electromagnetic spectrum weapons to suppress or deceive enemy electronic equipment. PLA EW strategy focuses on radio, radar, optical, infrared and microwave frequencies, in addition to adversarial computer and information systems. The Chinese see EW as an important force multiplier and would likely employ it in support of all combat arms and services during a conflict. PLA EW units have conducted jamming and anti-jamming operations, testing the military's understanding of EW weapons, equipment, and performance, which helped improve their confidence in conducting force on force, real equipment confrontation operations in simulated EW environments.

PLA strategists regard the ability to utilise space and deny adversaries access to space as central to enabling modern, information warfare.

*(Maj Gen PK Mallick, VSM (Retd.) has been a Senior Directing Staff (SDS) at National Defence College, New Delhi. He is an expert in Cyber Warfare, SIGINT and Electronic Warfare.)

Although PLA doctrine does not appear to address space operations as a unique operational "campaign," space operations form an integral component of other PLA campaigns and would serve a key role in enabling A2/AD (anti access / area denial) operations.

PLA has increasingly moved toward an operational construct that blends cyberspace operations with kinetic operations, creating a form of "cyber-kinetic strategic interaction." The goal would be to blind, disrupt or deceive adversary C4ISR systems while almost simultaneously deploying its formidable conventional strike, ballistic missile, and maritime power projection forces. The PLA envisions this operational concept as "integrated network electronic warfare," described by Michael Raska as the "coordinated use of cyber operations, electronic warfare, space control, and kinetic strikes designed to create 'blind spots' in an adversary's C4ISR systems."

The PLA has recently described this as a form of "network swarming attacks" and "multi-directional manoeuvring attacks" conducted in all domains – space, cyberspace, ground, air, and sea. The Strategic Support Force has been designed to provide these integrated operations, employing electronic warfare, cyberspace operations, space and counter-space operations, military deception and psychological operations working jointly with long-range precision strike, ballistic missile forces and traditional conventional forces.

Three Warfare and information Warfare

To set the strategic stage of the conflict, the "Chinese People's Liberation Army Political Work Regulations" which were promulgated in 2003, sets forth among the tasks of political work, the task of the "three warfares" — psychological warfare, public opinion warfare, and legal warfare.

- Psychological Warfare seeks to undermine an enemy's ability to conduct combat operations through operations aimed at deterring, shocking, and demoralising enemy military personnel and supporting civilian populations.
- Media Warfare is aimed at influencing domestic and international public opinion to build support for China's military actions and dissuade an adversary from pursuing actions contrary to China's interests.
- Legal Warfare uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended to build international support and manage possible political repercussions of China's military actions.

The PLA's operational hierarchy of combat consists of three major levels: war, campaigns and battles, each of which is informed, respectively, by a distinct level of operational guidance – namely strategy, campaign methods, and tactics. Three Warfares can be identified primarily as a campaign method with secondary, mostly strategic but also tactical applications. The PLA's combination of psychological warfare; the manipulation of public opinion, or media warfare and the manipulation of legal arguments to strengthen China's diplomatic and security position, or what China calls "legal warfare," join together in a comprehensive information operations doctrine.

C4ISR

As per the US DoD 2016 report, China continues to prioritise C4I modernisation as a response to trends in modern warfare that

emphasise the importance of rapid information sharing, processing and decision-making. The PLA seeks to modernise itself both technologically and organisationally to command complex, joint operations in near and distant battlefields with increasingly sophisticated weapons.

The PLA views technological improvements to C4I systems as essential to improve the speed and effectiveness of decision-making while providing secure and reliable communications to fixed and mobile command posts. The PLA is fielding advanced automated command systems like the Integrated Command Platform (ICP) to units at lower echelons across the force. The adoption of the ICP enables multi service communications necessary for joint operations. These C4I advancements are expected to shorten the command process. The new technologies introduced into the PLA enable information sharing — intelligence, battlefield information, logistical information, and weather reports on robust and redundant communications networks, to improve commanders' situational awareness. In particular, the transmission of ISR data in near real-time to commanders in the field could facilitate the commanders' decision-making processes and make operations more efficient.

These technical improvements have greatly enhanced the PLA's flexibility and responsiveness. "Informationised" operations no longer require in person meetings for command decision making or labor intensive processes for execution. Commanders can issue orders to multiple units at the same time while on the move and units can rapidly adjust their actions through the use of digital databases and command automation tools. The PLA also seeks to improve its C4I capabilities by reforming its joint command institutions at the national and regional levels.

Strategic Support Force (SSF)

The PLA Strategic Support Force (PLASSF) was created on 31 December 2015 as a newest branch of the People's Liberation Army (PLA). Introduced as part of China's military organisational reform, the PLASSF is not a full service branch, but an independent service arm under the direct leadership of the Central Military Commission (CMC). SSF is responsible for the PLA's space, cyber, and electronic warfare missions. Functionally and structurally, the SSF operates like the former Second Artillery Force and is an umbrella entity for electronic, information, and cyber warfare. This reform postures the PLA to conduct "local wars under informationised conditions" in support of its historic mission to "secure dominance" in outer space and the electromagnetic domain. Network (or cyberspace) forces are now alongside electromagnetic, space, and psychological operations forces and better organised to conduct integrated operations jointly with air, land, and sea forces. The establishment of the SSF disrupts traditional roles, relationships, and processes. It also disrupts power relationships within the PLA and between the PLA and the CCP. It challenges long-held organisational concepts, and is occurring in the midst of other landmark reforms, to include the establishment of new joint theatre commands. However, if successful, it would improve information flows in support of joint operations and create a command and control organisation that can develop standard operating procedures, tactics, techniques, procedures, advanced doctrine, associated training, along with driving research and development toward advanced capabilities. The force appears to have a staff department, equipment department, political department, and, presumably, a logistics department. More operationally, the force appears

to have headquarters components for its space and cyber forces, embodied in the Space Systems Department (SSF-SSD) and Network Systems Department (SSF-NSD) respectively. The SSF may create or may already have an Electronic/ Electromagnetic Systems Department (ESD) for its electronic warfare force.

SSF will be composed of three separate forces or force-types: space troops, cyber troops and electronic warfare forces. The cyber force would be composed of "hackers focusing on attack and defence," the space forces would "focus on reconnaissance and navigation satellites," and the electronic warfare force would focus on "jamming and disrupting enemy radar and communications." This would allow the PLA to "meet the challenges of not only traditional warfare but also of new warfare centred on new technology" (Global Times, January 16, 2017).

The SSF will draw from forces previously under the General Staff Department's (GSD) subordinate organs, to include portions of the First Department (1PLA, operations department), Second Department (2PLA, intelligence department), Third Department (3PLA, technical reconnaissance department), Fourth Department (4PLA, electronic countermeasure and radar department), and Informatisation Department (communications).

If information is power, then the GSD Third Department represents one of the most powerful bureaucracies in China today. Among its sources of strength is the country's largest pool of well trained linguists specialised in niche areas, such as banking and financial transactions, military activities, energy and diplomatic exchanges. The combination of Signals Intelligence (SIGINT) and Computer Network Exploitation, fusing transcripts of phone conversations with intercepted email exchanges, would enable a powerful understanding of plans, capabilities and activities of an organisation or individual in near real time. Key word and voice recognition technology and large data bases permit greater efficiency in collection directed against specific targets. Advanced computing facilitates breaking of all but the most sophisticated encryption and passwords. The linkage between CNO and PLA psychological warfare training units appears reasonable. Monitoring of communications, email accounts, websites, and internal networks could support sophisticated perception management operations. SIGINT, or technical reconnaissance in PLA lexicon, advances the interests of the Chinese Communist Party (CCP) and the People's Republic of China (PRC).

The PLA's SIGINT community consists of at least 28 technical reconnaissance bureaus (TRBs). The GSD Third Department has direct authority over 12 operational bureaus, three research institutes, and a computing centre. Eight of the 12 operational bureau headquarters are clustered in Beijing. Two others are based in Shanghai, one in Qingdao, and one in Wuhan. Ten additional TRBs provide direct support to the PLA's seven military regions (MRs), while another six support the PLA Navy (PLAN), Air Force (PLAAF), and Second Artillery Force (PLASAF).

Organizations Associated With Computer Network Defense

- PLA's Information Engineering University is the Third Department's training vehicle.
- PLA Communications Security Bureau China.
- North Computation Center Third Department Computing Center .
- National Research Center for Information

Security Technology (Network Risk Assessment).

- PLA Information Security Evaluation and Certification Center.
- Information Security Research Institute National Information Center (affiliated with science and technology equipment)
- National Information Security Engineering Technology Center.

Organization of the Operational Bureaus of the Third Department.

- 1st Bureau (61786 Unit) — decryption, encryption, information security.
- 2nd Bureau (61398 Unit) — US and Canada focus.
- 3rd Bureau (61785 Unit) — line of sight radio communications, direction finding, emission control.
- 4th Bureau (61419 Unit) — Japan and Korea focus.
- 5th Bureau (61565 Unit) — Russia focus.
- 6th Bureau (61726 Unit) — no mission given; Wuhan U. network attack and defense center is located in this area of operation.
- 7th Bureau (61580 Unit) — some computer network attack and computer network defense, some work on the US network-centric concept, psychological and technical aspects of reading and interpreting foreign languages.
- 8th Bureau (61046 Unit) — Western and Eastern Europe, Middle East, Africa, Latin America.
- 9th Bureau (unknown Unit) — strategic intelligence analysis/data base management, the most opaque bureau.
- 10th Bureau (61886 or 7911 Unit) — Central Asia or Russia, telemetry missile tracking, nuclear testing.
- 11th Bureau (61672 or 2020 Unit) — Russia.
- 12th Bureau (61486 Unit) — satellites, space-based signals intelligence (SIGINT) collection.

Western Theatre Command (WTC)

After the modernisation the WTC has emerged as the largest theatre and has complex terrain including desert and high mountains, long borders and challenging social conditions. Theatre missions include supporting the People's Armed Police Force maintaining internal stability in the restive Tibet and Xinjiang regions. Disaster relief requiring liaison with civilian organisations is also an important theatre mission. External responsibilities include responding to possible unrest in Central Asia under the auspices of the Shanghai Cooperation Organisation (SCO). However, the WTC's primary strategic direction is India and the contested border regions (Xinhua, August 18, 2014; China Military Online, March 3, 2016).

Tibet Military Command/Military District in the WTC has been elevated by one level compared to other provincial level military districts and placed under the PLA Army (PLAA). An article in The Global Times reported that the Tibet Military Command will be responsible for operations against India, at least in the Arunachal Pradesh area, training forces for specialised high-altitude mountain warfare and long-range mobility for such a contingency (Global Times, May 13, 2016). However, Army command would appear to usurp the theatre's command responsibility. The Xinjiang Military District is also under PLAA command. The current reforms and reorganisation make the services responsible for force development and

training their respective forces, which would appear to include the Army commands in the Tibet and Xinjiang Military Districts. Since the WTC has a difficult internal mission, the Army might additionally be responsible for internal missions in Tibet and Xinjiang, acting as an intermediate command level for the theatre, which would have a daunting span of control if widespread unrest occurred in both areas, compounded by an external crisis.

The WTC headquarters includes a joint operations command centre also located in Chengdu. The theatre Army Headquarters is in Lanzhou. The new Strategic Logistics Support Force has subordinate Joint Logistics Support Centres in each theatre, with one in Xining for the WTC. The WTC can deploy subordinate PLAA and PLAAF units, and request additional forces from the CMC if required.

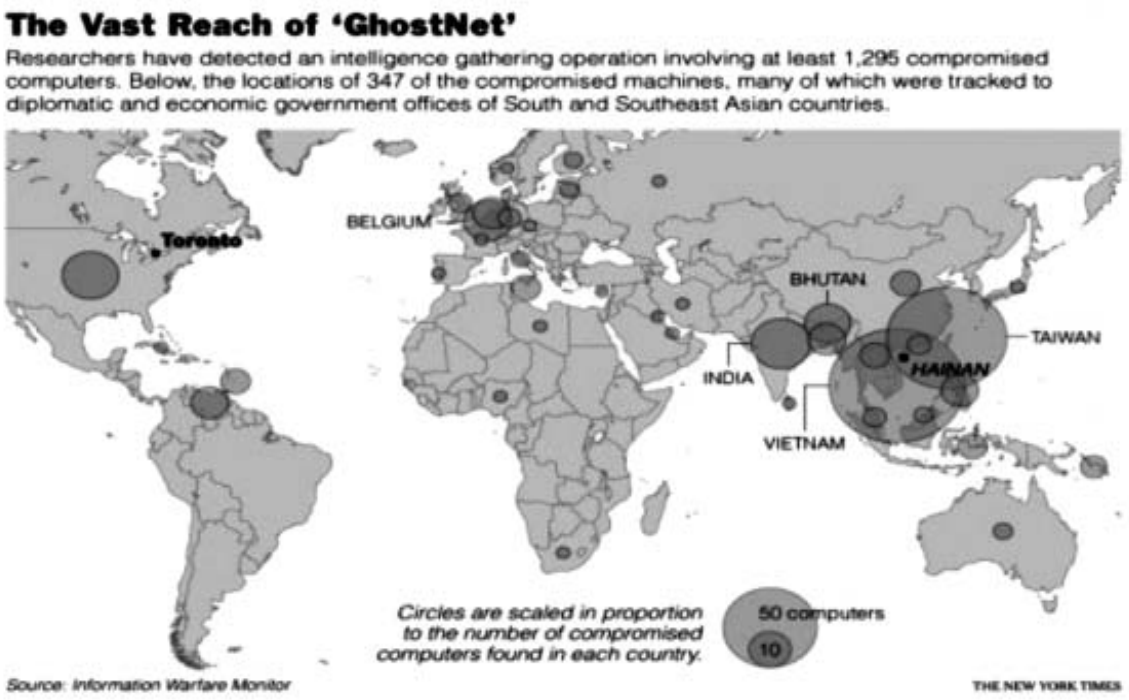
The WTC would have to coordinate operations with the responsible command for naval operations against India. The WTC focuses on relevant campaign scenarios to train troops for potential combat operations. PLA publications detail several campaigns that the WTC could conduct including antiterrorism, stability maintenance operations to combat internal unrest; joint border counterattack campaigns to defend against an attack and regain lost territory; mountain offensive campaigns; and joint fire strike campaigns usually supporting another campaign, but also an independent campaign (Global Times, September 5, 2012).

GhostNet

China has been conducting cyber operations against India for a long time. One of the earlier examples was the GhostNet episode.

Ross Anderson, at Cambridge University, and Shishir Nagaraja at the University of Illinois, wrote: "The office of the Dalai Lama started to suspect it was under surveillance while setting up meetings between His Holiness and foreign dignitaries. They sent an email invitation on behalf of His Holiness to a foreign diplomat, but before they could follow it up with a courtesy telephone call, the diplomat's office was contacted by the Chinese government and warned not to go ahead with the meeting." Between June 2008 and March 2009, the Information Warfare Monitor conducted an extensive and exhaustive two phase investigation focused on allegations of Chinese cyber espionage against the Tibetan community. GhostNet, had penetrated 103 countries and infected at least a dozen new computers every week. This global web of espionage has been constructed in two years. The research team found a wide-ranging network of compromised computers. This extensive network consisted of at least 1,295 infected computers in 103 countries. Significantly, close to 30% of the infected computers could be considered high value and include the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organisations; and an unclassified computer located at NATO headquarters.

The GhostNet system directed infected computers to download a Trojan known as ghost RAT that allowed attackers to gain complete real time control. These instances of ghost RAT were consistently controlled from commercial Internet access accounts located on the island of Hainan, People's Republic of China. GhostNet was capable of taking full control of infected computers,



including searching and downloading specific files and covertly operating attached devices, including microphones and web cameras.

The Key Findings of the investigation were :

- GhostNet infected at least 1,295 computers in 103 countries, of which close to 30% can be considered as high value diplomatic, political, economic and military targets.
- GhostNet penetrated computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets.
- Documentation and reverse engineering of the modus operandi of the GhostNet system including vectors, targeting, delivery mechanisms, data retrieval and control systems revealed a covert, difficult to detect and elaborate cyber-espionage system capable of taking full control of affected systems.

Conclusion

China has developed its electro magnetic warfare capabilities keeping in mind USA as its main adversary. It has very judiciously concentrated on those specific aspects which it thought would give it asymmetric advantage. China is still well behind USA in electro magnetic battlefield, but it is catching up. However, against India it has massive advantage. China has already undergone drastic changes in its doctrine and concept of warfare, organisation, training, human resource management and financial allocation in niche technology areas. Government of India and Indian armed forces must move fast to confront China in electromagnetic battlefield in any eventual conflict scenario. At this present juncture India has much to do to catch up.

◆◆◆

OPINION

Global Health Diplomacy: A Strategic Opportunity for India

Shantesh Kumar Singh*

Introduction

With the increasing crisis and challenges to human security, challenging the basic nature of life of people, governments and international institutions have started seeking methods to redefine international politics and foreign policy making. However, the challenges have been multifaceted, which has scarred every sphere of human life. The challenges to human rights and life unfolding daily in the Middle East, which is spreading fast in the entire region demands bold new initiatives. The concept of security has shifted, moving away from a macro focus solely on the security of nations and other large entities to also include a micro-level focus on the security of individuals and communities, in which securing the standard of health and protecting life has been one of the primary concerns. In the recent years, health has been adapted as a strategic foreign policy and diplomatic concern for many countries and regions of the world.[1]

However, such shift is not a new phenomenon. For example, the Red Cross doctrine of the 1860s clearly states the security of the people, and those elements of the doctrine were institutionalised in the UN Charter of the 1940s as the Universal Declaration of Human Rights and the Geneva Conventions.[2] The Foreign Policy and Global Health Initiative, launched by the foreign ministers of Brazil, France, Indonesia, Norway, Senegal, South Africa and Thailand in 2006 and articulated in the Oslo Ministerial Declaration in 2007, is one of the most well-known efforts to integrate health issues into foreign policy, making health a determinant in diplomatic parlance. In the declaration it was stated:

We believe that health is one of the most important, yet still broadly neglected, long-term foreign policy issues of our time...We believe that health as a foreign policy issue needs a stronger strategic focus on the international agenda. We have therefore agreed to make 'impact on health' a point of departure and a defining lens that each of our countries will use to examine key elements of foreign policy and development strategies, and to engage in a dialogue on how to deal with policy options from this perspective.[3]

A definition for global health diplomacy has been much discussed and debated. Definitions range from normative, "an emerging field that addresses the dual goals of improving global health and bettering international relations"[4], or "winning hearts and minds of people in poor countries by exporting medical care, expertise and personnel to help those who need it most"[5] to a more technical, "multi–level, multi–actor negotiation processes that shape and manage the global policy environment for health".[6]

In particular, Fidler and Nick Drager stated

Dr. Shantesh Kumar Singh is currently working as a Postdoctoral Fellow at the International Institute for Global Health, United Nations University, Kuala Lumpur, Malaysia and he also holds a regular faculty position in the Department of Political Science at Shaheed Bhagat Singh College, University of Delhi, Delhi, India.

that it is the increasing frequency of crisis situations with profound health impacts and high economic costs which involves immunisation against major diseases along with providing proper food and drinkable water and health facilities to conflict and remote and less developed areas, along with meeting the challenge of countering diseases that travels beyond borders, such as polio, anthrax, SARS, HIV/AIDS and pandemic flu that have made health a key pillar of the foreign policy agenda. They argue that health problems that do not have the uncertainty of a potentially catastrophic event, such as non-communicable diseases, neglected tropical diseases, road traffic injuries, mental health, and maternal and child health do not pose any immediate danger to non-affected states and give no incentives for foreign policy action. Foreign policy attention is thus largely given to issues that reflect interdependence since governments seek collective action for self-protection. Fidler further observes with Lawrence Gostin that "the biosecurity threats present in our globalized world actually make self-help the most attractive and effective strategy for powerful states".[7] Andrew Price-Smith concurs with Fidler that interdependence between states resulting from the processes of globalization has pushed developed countries to become interested in the health situation in developing countries.[8] Price-Smith explains health's increased importance in foreign affairs as directly linked to the security implications of contemporary health threats. He draws particular attention to the effects of infectious diseases on destabilization of states and the ensuing terrorism, criminal activity and illicit trade which have harmful effects on the global scale.[9] Large scale immigration, failure of state machineries and regional conflicts also pose a major challenge to health care. Health is on the radar of foreign policy because it has become integral to three global agendas:

1. **Security** — driven by the fear of global pandemics or the intentional spread of pathogens and an increase in humanitarian conflicts, natural disasters, and emergencies;
2. **Economic** — concerned not only with the economic effect of poor health on development or of pandemic outbreaks on the global market place but also the gain from the growing global market in health goods and services;
3. **Social justice** — reinforcing health as a social value and human right, supporting the United Nations millennium development goals, advocating for access to medicines and primary health care, and calling for high income countries to invest in a broad range of global health initiatives.[10]

Intellectual property is one of the vital facets that face health practitioners and one of the main issues where health and foreign policy intersect. It is also the area where health concerns have been most successfully integrated into economic policymaking.

The concept of "medical diplomacy" was introduced as early as 1978 by Peter Bourne, special assistant to the president for health issues during the Carter administration, USA. According to GHS Initiative in Health Diplomacy, UCSF (2008), "Health Diplomacy occupies the interface between international health assistance and international political relations. It may be defined

as a political change agent that meets the dual goals of improving global health while helping repair failures in diplomacy, particularly in conflict areas and resource-poor countries."[11] More recently, the July 2011 BRICS (Brazil, Russia, India, China, and South Africa) health ministers meeting was held in Beijing with the theme of "Global Health — Access to Medicine", where ministers pledged to work together to implement health reforms and share the successes and challenges of experiences.

"In the past" — said Robert Cooper, "it was enough for a nation to look after itself. Today it is no longer sufficient."[12] This is particularly true in the health arena. There is an increasing range of health issues that transcend national boundaries and require action on the global forces that determine the health of people. The broad political, social and economic implications of health issues have brought more diplomats into the health arena and more public health experts into the world of diplomacy.[13]

India and Health Diplomacy

Being a recent arena of diplomacy, Indian diplomats and foreign policy practitioners have started growing an understanding and developing India's diplomatic initiatives in the health sector. Most of the global health initiatives originate in the United Nations and under the aegis of the World Health Organisation (WHO). Many countries have added a full-time health attaché to their diplomatic staff in recognition of the importance and complexity of global health deliberations; others, along with India, have added diplomats to the staff of international health departments. Their common challenge is to navigate a complex system in which issues in domestic and foreign policy intertwine the lines of power and constantly influence change, and where increasingly rapid decisions and skillful negotiations are required in the face of outbreaks of disease, security threats or other issues.

New global health problems include infectious diseases, non-communicable diseases (NCDs), bioterrorism and dual-use research, health-system strengthening, and critical social determinants of health, such as food security. These health threats have led to the emergence of new actors, processes, and institutions seeking to mitigate their effects.

Although progress has been made in disease prevention and control, as well as in health-system strengthening, more still needs to be done to continue the fight against HIV/AIDS, manage biosecurity issues and acute pandemics, and ensure effective and sustainable global health financing. Financing is a particular worry during times of austerity.[14] With the dynamism brought into foreign policy decision making in India, health is turning into a major fulcrum which will be playing a major determinant in building relations between nations. India has started playing an integral role in global health assistance, making it an integral part of India's foreign assistance program and its significance is growing exponentially over the years. Indian policymakers believe the scope of the country's health assistance program will continue to expand and hopeful of exploring opportunities for country's private health sector and civil society in health assistance initiatives. Health assistance can be traced through infrastructure, human resources, education and capacity building. Health assistance can typically be seen in the form of bilateral health assistance,

Health IT and Pharma etc. Since 2009, India has committed at least US$100 million to bilateral health projects in nearly 20 countries in south Asia, southeast Asia and Africa. India's Health IT could develop the Pan-Africa Telemedicine and Tele-Education Network, where hospitals and universities throughout Western Africa are being linked with counterparts in India to facilitate sharing best medical practices.[15]

The foreign policy and policymakers in India are committed to strengthening cooperation and sharing of experiences in public health sector. India uses foreign assistance as diplomatic tool for foreign trade and investment; and sustained cooperation to many developing and under-developed nations including Africa. India strongly believes in the concept of south-south cooperation and critical about western donor-aid concept. Indian foreign assistance typically includes technical cooperation, grants, and contributions to international organizations, soft loans, and Export-Import (EXIM) Bank lines of credit with subsidized interest rates.[16]

However, the role of India in healthcare should be explored for universal health coverage. India's engagement in global health diplomacy needs to be formulated and implemented not only to generate revenue but also to have an increased global political engagement. India cannot wait for a pandemic to occur, like (SARS, CHAGAS, EBOLA and ZICA) to reexamine and develop a comprehensive foreign policy which strongly encompasses the principle of health security.

There is a need to build capacity for global health diplomacy by training public health professionals and diplomats respectively. Two types of imbalance need to be addressed as a priority: imbalances that can emerge between foreign policy and public health experts, and imbalances that exist in the negotiating power and capacity between developed and developing countries. The linking of health and foreign policy has revealed substantive tensions between the two fields. At their most fundamental level, public health and foreign policy communities differ in their ideologies, functions, audiences and obligations, as well as approaches to solving problems.[17] Yet despite these differences, health issues have featured in foreign policy circles with increasing frequency.

Economically, sustaining health prominently in foreign policy is becoming more difficult because the international economic context and domestic fiscal crises adversely affect governments, societies, international organizations and non-state actors. In many ways, the life-blood of the rise of health within foreign policy has been the massively increased funding for global health, which went from $5.59 billion in 1990 to $21.79 billion in 2007.[18] In epidemiological terms, foreign policy action will become harder because, as noted above, political and economic capital for existing efforts (e.g. HIV/AIDS) – widely recognized as inadequate – will be more scarce, forcing tough decisions about how to prioritize available political commitment and economic resources.[19] Especially for a country like India, which is geo-strategically located in a neighbourhood, which has polio on the rise, affected by massive natural calamities on a yearly basis, suffering from malnutrition and lack of proper governance in tackling such major health challenges.

There is a large reservoir of highly trained experts and scientists in knowledge based industries, such as, information technology, science, research and development etc. They can play an important part in developing India as a Research & Development centre. The overseas Indians have distinguished themselves in the field of medicine and healthcare in the countries of their residence. They can play an important role in secondary and tertiary healthcare in India. The Diaspora can also help in promoting India as healthcare destination. They can effectively contribute in the expansion and growth of pharmaceutical industry.[20] The faster Indian foreign policy institutions adapt using as an integral element in their decision making apparatus, it would not only register as an altruistic behaviour of the state machinery, but a strategic move to bring regional and sub regional integration, along with creating a global forum to having an integrative mechanism to be responsive not only during times of exigency but to be apt in adapting with the changing global health necessities. While upholding the international standards of health, and maintaining the solemn path of sticking to serving to the maximum number of masses in need of being provided health security, one can take the assistance of "policy entrepreneurs" within governments which function not only in the sphere of being public health officials, but as health ambassadors for the country, which would provide a definitive direction for having a national health policy that would be strengthened by the nation's foreign policy approach.

References:

[1] *Fidler, D., (2005), Health and foreign policy: a conceptual overview. London: The Nuffield Trust; Fidler, D., 2006. Health as foreign policy: harnessing globalization for health. Health Promotion International, 21(Supplement 1): 51-58; Kickbusch, I., 2008. Moving Global Health Governance Forward. In: K. Buse, W. Hein and N. Drager, eds. Making Sense of Global Health Governance: A Policy Perspective. Basingstoke: Palgrave Macmillan, 320-339.*

[2] *Paula Gutlove and Gordon Thompson, (2003), "Human Security: Expanding the Scope of Public Health," in Medicine, Conflict & Survival, 19, pp. 17-34.*

[3] *Amorim, C., Douste-Blazy, P., Wirayuda, H., Støre, J.G., Gadio, C.T., Dlamini-Zuma, N., and Pibulsonggram, N., (2007), Oslo Ministerial Declaration—global health: a pressing foreign policy issue of our time. The Lancet, 369 (9570): 1373-1378*

[4] *Adams, V. (2008), Global health diplomacy. Medical Anthropology, 27(4), pp. 315-323*

[5] *Fauci, A. (2007). The expanding global health agenda: A welcome development. National Medicine, 13, 1169-1171*

[6] *Kickbusch, I., et al. (2008), Global health diplomacy: The need for new perspectives, strategic approaches and skills in global health. Geneva: World Health Organization, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2636243/*

[7] *World Health Organisation, (2009), Global Health and Foreign Policy: Strategic Opportunities and Challenges. Background Paper for the Secretary-General's Report on Global Health and Foreign Policy. Geneva: WHO*

[8] *Gostin, L. and Fidler, D., (2006), Biosecurity under the Rule of Law. Case Western Reserve Journal of International Law, 38: 437-478; Price-Smith, A., 2009. Contagion and chaos: disease, ecology, and national security in the era of globalization. Cambridge, Mass.: The MIT Press.*

[9] *Price-Smith, A., (2002), The health of nations: infectious disease, environmental change, and their effects on national security and development. Cambridge, Mass.: The MIT Press*

[10] *Ilona Kickbusch, "Global health diplomacy: how foreign policy can influence health",* The British Medical Journal*, 2011;342:d3154 doi: 10.1136/bmj.d3154, http://graduateinstitute.ch/files/live/sites/iheid/files/sites/globalhealth/shared/1894/Publications/global%20health%20diplomacy_how%20foreign%20policy%20can%20influence%20health_bmj.d3154.full.pdf*

[11] *UCSF Global Health Sciences, "GHS Initiative in Health Diplomacy.", http://globalhealthsciences.ucsf.edu/programs/Diplomacy.aspx*

[12] *Cooper R., (2003), The breaking of nations. Order and chaos in the 21st century. New York: Atlantic Monthly Press;*

[13] *Ilona Kickbusch, Gaudenz Silberschmidt, and Paulo Buss, (2007), "Global health diplomacy: the need for new perspectives, strategic approaches and skills in global health",* Bulletin of the WHO*; 85(3): 230–232*

[14] *Yanzhong Huang, (2013), "Enter the Dragon and the Elephant: China's and India's Participation in Global Health Governance",* Council on Foreign Relations: International Institutions and Global Governance Program*, Working Paper, (2013), pp. 3-4, https://assets.documentcloud.org/documents/682681/enter-the-dragon-and-the-elephant.pdf*

[15] *Raghavendra Madhu and Srikanth Reddy, (2014) "An Opportune time for India to play the Global Health Diplomacy Card",* Global Policy*, September 22, http://www.globalpolicyjournal.com/blog/22/09/2014/opportune-time-india-play-global-health-diplomacy-card*

[16] *Raghavendra Madhu and Srikanth Reddy, (2014), "An Opportune time for India to play the Global Health Diplomacy Card",* Global Policy, *http://www.globalpolicyjournal.com/blog/22/09/2014/opportune-time-india-play-global-health-diplomacy-card*

[17] *Feldbaum, H., Patel, P., Sondorp, E., and Lee, K., (2006), Global health and national security: the need for critical engagement. Medicine, conflict, and survival, 22 (3): 192-198.*

[18] *Institute for Health Metrics and Evaluation, Financing Global Health: Development Assistance and Country Spending in Uncertainty (Seattle: Institute for Health Metrics and Evaluation, 2010), p. 15*

[19] *David P. Fidler, "Assessing the Foreign Policy and Global Health Initiative: The Meaning of the Oslo Process", Briefing Paper,* Chatham House*, (2011), GH BP 2011/01, p. 14, https://www.chathamhouse.org/sites/files/chathamhouse/0611bp_fidler.pdf*

[20] *J. C. Sharma, (2013), "India's Foreign Policy, National Security & Development", Distinguished Lectures*, Ministry of External Affairs*, http://www.mea.gov.in/foreign-policy.htm*

◆◆◆

India China Standoff: How and Why

Apoorva Goel*

On 6 June 2017, ahead of the start of the SCO summit in Astana in Kazakhstan, a meeting took place between Prime Minister Narendra Modi and President Xi Jinping of China. The meeting, coming on the heels of a series of contentious issues between the two countries was cordial, giving rise to the hope of smoothening of diplomatic relations. The preceding months had seen a distinct cooling of relations, with Beijing continuing to block New Delhi's bid seeking membership of the Nuclear Suppliers Group, stonewalling India's attempts to sanction JeM chief Masood Azhar at the UN and renaming places in Arunachal Pradesh. India, on its part, boycotted China's high-profile Belt and Road Forum held in Beijing in May, in which 29 world leaders took part, much to the former's chagrin, as the China-Pakistan Economic Corridor (CPEC), which is an important constituent of the project, passes through Indian territory illegally occupied by Pakistan.

The meeting on the sidelines of SCO summit, however, flattered to deceive. Within ten days, on 16 June 2017, a Chinese road-construction party with heavy equipment, accompanied by soldiers of the People's Liberation Army (PLA) of China, intruded into the Dolam plateau and started work on extending an unmetalled track in Bhutanese territory. Personnel from the Bhutanese Army who arrived at the scene found themselves unable to stop the Chinese, subsequent to which troops from the Indian Army moved into the area, and stopped the road construction. The face-off between the Chinese and the Indian troops has continued thereafter, with neither side prepared to budge from their position.

The area in contention — the Dolam plateau — is however Bhutanese territory, though China lays claims to it, based on their interpretation of an Anglo-Chinese convention of 1890. Bhutan was however not a signatory to the above convention, which in any case has been overtaken by later day agreements with Bhutan of 1988, 1998 and 2012, which clearly advocate the maintenance of status quo in the disputed areas till the issues are resolved through dialogue. More than two dozen meetings have taken place between Bhutan and China on this issue without making any headway. China's attempt to build a road through the Dolam plateau is thus an attempt to change the status quo and is in violation of the agreements between Bhutan and China.

An understanding of the geography of the place is important to grasp the ground situation. The Chumbi Valley in this region forms a wedge into India, with Sikkim to the West and Bhutan to the East. The trijunction between India, Bhutan and Tibet in this region is at Batang La. South of Batang La is the Indian post Doka La. Further South, about 6.5 km from Batang La is Gymochen, which China claims as the trijunction and on which it bases its

Apoorva Goel is working as a research intern with India Foundation. She is pursuing her B.Com (Hons.) from Shri Ram College of Commerce, New Delhi. This article has been written with inputs from Maj Gen. Dhruv C. Katoch)

claim to the Dolam plateau. To the East of Gymochen runs the Jampheri ridge, a feature of great strategic significance, which India and Bhutan believe China is having an eye on. As per the agreement between the Special Representatives of India and China in 2012, the two sides have to maintain the status quo until their competing claims are resolved in consultation with the third party, which in this case is Bhutan. Gymochen is 20 km crow flight distance from the West Bengal border.

North East of Doka La, is another feature called Doklam, which has no contiguity with India and which must not be confused with the Dolam plateau. The Doklam plateau is about 30 km away from the stand off point at Dolam, near Doka La. The Indian Ministry of External Affairs and the Embassy of Bhutan in New Delhi refer to the location of the standoff as the Dolam plateau, which is in the Doklam area.

India is rightly concerned with the Chinese attempts at unilaterally altering the status quo. From southern tip of the Chumbi Valley, Jalpaiguri is but 99 km crow flight distance. This makes India extremely vulnerable as the entire Northeast India can be cut off from this point. Chinese build up in this region is dependent on road communications. The Chinese have built a class 60 road from Lhasa to Gyantse, which extends deeper inside the Chumbi Valley. Several unmetalled tracks emanate from there, one of which comes up to a point close to Doka La. This 20 km long track is classified as a class-5 track, meaning it can take light vehicles. At the end of this 20 km track, is a "turning point", a wider area where large vehicles can reverse and return. This turning point is a few metres away from the Indian Army post at Doka La, around 3.5 km short of Gymochen, and approximately 3 km from Batang La and is the place of the present standoff between the two countries. Chinese attempts to extend the road network in Bhutanese territory pose a threat to India which India will be naive to allow, especially as such an attempt amounts to altering of the status quo, which till now has helped to maintain peace in the area. Chinese military patrols have been regularly coming up to the turning point on the Class 5 track. Chinese graziers often come up to the Torsa Nala. Chinese military patrols have also been known to go almost up to the Jampheri ridge, but this is rare. In a sense, while the de jure border is aligned with Batang La, the de facto border has been at Doka La.

The last three years under the NDA government have seen a markedly different Indian government, which is willing to protect its interests. India's diplomatic outreach to strengthen its ties with the US, Japan, South Korea and Israel marks a major shift from earlier years when India was content to remain a backroom player. To this end, India's efforts to get into the nuclear club and to the UN's highest decision-making body are a work in progress.

The Indian focus on revitalising its economy is proceeding apace, with India now the fastest growing economy in the world, displacing China from the top spot. While India is still far from competing with China in the economic and military sphere, it remains a challenge to China to achieve

regional hegemony, in line with a Chinese saying that one mountain can have only one tiger. That role China has abrogated for itself, which brooks no space for any other. Indian absence from the Chinese Road and Belt project thus was not viewed favourably by China, which expected India to fall in line with its initiative. This explains consistent Chinese attempts to give support to Pakistan and to obstruct India's entry into the Nuclear club and to the UN Security Council.

So, what of the future? While both sides have agreed to a troop withdrawal on 28 August, thus deescalating the current inpase, India-China relations are fed by wider geo-strategic concerns. In the instant care, China has upped the ante by closing the pilgrims route to Mansarovar via Nathu La pass and through its state controlled Global Times paper, issued veiled threat to India that it could review its policy on Sikkim and Bhutan. this ofcourse could have led to giving India the option to reexamine its position on Tibet, which in any case was an independent kingdom and acted as a buffer between India and China.

While a conflict on a localised issue will benefit no one, least of all India and China, it is incumbent on the part of the Chinese to respect Indian sensitivities in the area and to adhere to the rule of law. For India, the best remedy to avoid war is to show the will and the resolve to fight for the preservation of Bhutan's territorial integrity.

◆◆◆

Three Warfares: A Prong of China's Military Strategy

Dhruv C Katoch*

Amid the faceoff between India and China over the Dolam plateau — an area which belongs to Bhutan but is claimed by China — an understanding of Chinese military strategy throws up light on the current aggressive and threatening posture taken up by the Chinese media over an issue which normally would not invite such rhetoric. The People's Liberation Army (PLA) of China has closely observed how the United States has conducted its wars over the past two decades, both in Afghanistan and in the Gulf, and its military doctrine has been greatly influenced by the impact of technology and communications on the battle field. This has influenced to a large extent, the approaches to what China first termed 'Local Wars Under Modern, High-Tech Conditions', and are now calling 'Local Wars Under Informationalized Conditions'. PLA theorists and planners believe future campaigns will be conducted simultaneously on land, at sea, in the air, in space, and within the electronic sphere. Preparation for conflict is based on the following premises:

- Future wars will be shorter, perhaps lasting only one campaign;
- Will almost certainly not entail the occupation of China, although Chinese political, economic, and military centres are likely to be attacked;
- Will involve joint military operations across land, sea, air, cyberspace and outer space, and the application of advanced technology, especially information technology.

Consequently, the modernisation of the Chinese military is focussed on preparing the PLA to fight and win short-duration, high-intensity conflicts along China's periphery. This includes scenarios for Taiwan, building counters to third-party, including potential US intervention in cross-Strait crises and Chinese claims along its borders with India. With an increase in its military capability, China has begun flexing its muscles throughout Asia, sometimes acting unreasonably. With India, its relationship could be described as stable at the strategic level but aggressive at the tactical level and the stand off at the Dolam plateau is proof of such behaviour.

PLA's Military Modernisation

PLA has been focussed on augmenting and expanding its force of ballistic missiles (long-range and short-range), cruise missiles, submarines, advanced aircraft, and other modern systems. The PLA is working toward these goals by acquiring new foreign and domestic weapon systems and military technologies, promulgating new doctrine for modern warfare, reforming military institutions, personnel development, enhancing professionalism and improving exercise and training standards. As of now however, China's ability to project conventional military power beyond its periphery remains limited. It thus advocates a policy of "Active defense" which posits a defensive military strategy and asserts that China does not initiate wars or fight wars of aggression, but engages in war only to defend national sovereignty and territorial integrity and attacks only after being attacked. Beijing's definition of an attack against its territory, or what constitutes an initial attack, is left vague, however. In the Indian context, an unresolved border dispute could well result in China

*Maj Gen Dhruv C Katoch is Director, India Foundation; Editor, SALUTE Magazine and former Director, Centre for Land Warfare Studies (CLAWS).

using force to reclaim territory which China claims and justify the action as self defence. Once hostilities have begun, evidence suggests the characteristics of "active defense" are distinctly offensive. Advances in military technology provide Beijing with an expanded set of limited force options. Chinese operational-level military doctrine defines these options as "nonwar" uses of force — an extension of political coercion and not an act of war. With growth in China's military power, we can expect Chinese leaders to resort to force or coercion more quickly to press diplomatic advantage, advance security interests, or resolve disputes.

While the military focus of China is primarily aimed at countering the United States, the capabilities and competencies so developed can in any event be used to resolve issues with India or any other of China's neighbours from a position of strength. As part of its war fighting strategy, the Chinese lay great stress on psychological operations in what they refer to as the 'Three Warfares'. This implies dictating the strategic terms of the conflict, by influencing domestic opinion, opposition will, and third-party support. This is what was played out on the Dolam plateau.

To set the strategic stage of the conflict, the "Chinese People's Liberation Army Political Work Regulations" which were promulgated in 2003, sets forth among the tasks of political work, the task of the "three warfares" — psychological warfare, public opinion warfare, and legal warfare. In the Indian context, this could be aimed to:

- Sap Indian will and thereby win without fighting.
- Attenuate alliances, thereby limiting foreign support.
- Reinforce domestic will.

Psychological warfare (xinlizhan), can occur at the tactical, operational, or strategic level. But, according to some PLA analyses, it is at the strategic level that psychological warfare may have the greatest impact, since it may undermine the enemy's entire will to resist. Psychological warfare at that level is aimed not only at an opponent's political and military leaders, but also at their broader population. It is also aimed at one's own population and leadership cohort, in order to strengthen the will to fight. Finally, it also targets third-party leaders and populations, in order to encourage support for one's own side, and discourage or dissuade them from supporting an opponent.

In order to generate such effects, Chinese writings suggest that psychological warfare, including its subordinate areas of public opinion and legal warfare, will often begin before the formal commencement of open hostilities and will operate not only in the military and diplomatic realms, but also the political, economic, cultural, and even religious arenas, which cannot easily be done on short notice.

Public opinion warfare (yulunzhan) refers to the use of various mass information channels, including the Internet, television, radio, newspapers, movies, and other forms of media, to generate public support both at home and abroad for one's own position and create opposition to one's enemy. In this view, public opinion is now a distinct, second battlefield, almost independent of the physical one. The ability to shape the narrative, so to speak, including establishing moral ascendancy and justification, requires long-term efforts.

Legal warfare (faluzhan) is the use of domestic law, the laws of armed conflict, and international law in arguing that one's own side is obeying the law, the other side is violating the law, and making arguments for one's own side in cases where there are also violations of the law. As an example, the Anti-Secession Law, passed on March 14, 2005, serves as a form of military deterrent/coercion (junshiweishe), through the use of legal

warfare. Efforts by Taiwan to secede would therefore violate this law, and would lead to punishing consequences.

Ultimately, the combination of the "three warfares" constitutes a form of defense-in-depth, but one that is executed temporally (in order to delay an opponent) and politically (by fomenting public disagreement and doubt), rather than physically. It is aimed not only at an opponent's leadership and public support, but also that of third parties. The goal remains anti-access/area denial; it is simply the means and the battlefields that have shifted. The above fits in with the Chinese concept as enunciated by Sun Tzu of winning without fighting.

While the present stand off is unlikely as of now to lead to a major conflict, it certainly is a tool being used by China to browbeat India into submission and at the same time, get world support for its action as being justified on legal grounds. This presents a unique challenge to India to maintain its position and standing in the comity of nations. The pressure tactics being employed by the Chinese need to be countered and along with that, the nation needs to be prepared for war, should such a contingency arise. While the focus of China's military modernisation in the near term appears to be preparing for potential conflict in the Taiwan Strait, analysis of Chinese military acquisitions also suggests the PLA is generating military capabilities that go beyond a Taiwan scenario and which have India as the possible adversary. The causative factors for conflict exist in an unresolved border between Tibet and India. China could also use war as a means to divert the attention of its people from domestic issues, to preserve the dominance of the Communist Party over the country. In case of conflict, the first step would in any case be setting up the strategic stage of the conflict, through the 'three warfares' — psychological warfare, public opinion warfare, and legal warfare. This may well be a year or two before the actual conflict, in the hope of achieving its aims without the need to take recourse to war. In case China's political aims are not achieved though the above, it could follow up with military actions, as under:

- Cyber attacks to hit at Indian financial and economic institutions.
- Exploiting the full range of space warfare capabilities to achieve space dominance.
- Concentrated SRBM attack, at key command and communication nodes.
- "Integrated Network Electronic Warfare" as described earlier along with limited kinetic strikes against key C4 nodes to disrupt Indian battlefield network information systems.

The Chinese would seek conflict termination at each stage of the escalatory ladder. Build up of troops in the Tibetan Plateau would take place simultaneously for ground action if the objectives have not been met by the means employed earlier. Thereafter, we could expect a conventional military conflict. From the Indian viewpoint, the conduct of a successful defensive battle would require negating Chinese actions at each stage. We would require very high capability in NCW, EW and space warfare. It is also essential that the IAF has dominance over the Tibetan plateau if a successful defensive battle is to be fought. Artillery voids need to be made up at the earliest and logistic capability enhanced to defeat any Chinese designs on our Northern and Eastern borders. The real threat is not from the number of divisions which the Chinese can amass but from enhanced capabilities which we need to match and surpass. This must include the domain of psychological warfare and perception management operations.

◆◆◆

REPORT

India-ASEAN Youth Summit 2017

Rohit Kumar

"India and ASEAN countries have a long history of cultural, social and economic interaction" - Atal Bihari Vajpayee, Former Prime Minister of India

The year 2017 holds a great significance to India as well as to the ASEAN member countries. It marks the 50th year of the formation of ASEAN and 25 years of Dialogue Partnership between India and ASEAN countries. India-ASEAN member countries have strengthened their bond since they have committed themselves to jointly contribute to the promotion of peace, stability and development in the Asia-Pacific region and have responded positively and mutually to global issues and challenges of dynamic regional and international environment. Another aspect of the relationship is the involvement of Youth in bringing mutual peace and stability in the India-ASEAN region.

To highlight the important role youth play in building this relationship, the first India-ASEAN Youth Summit was organised in Bhopal, Madhya Pradesh by India Foundation in association with Ministry of External Affairs, Government of India and Government of Madhya Pradesh. Youth Delegates from India and the ten ASEAN countries participated in the Youth Summit which comprised many panel and parallel discussions that addressed a wide range of topics. Speakers from all segments gave their valuable inputs to the gathering comprising of young delegates from India and ASEAN countries.

Day 1: August 14, 2017: Inaugural Session

The Inaugural session was chaired by Shri Shivraj Singh Chouhan, Chief Minister of Madhya Pradesh. The Chief Guest for the Inaugural session was Gen V. K Singh, Minister of State for External Affairs, Government of India and the Guest of

Honour was Ms Preeti Saran, Secretary (East), Ministry of External Affairs, Government of India.

While addressing the gathering, Ms Preeti Saran, introduced the theme "Shared Values Common Destiny" to the gathering and also stated the importance of having a stable relationship in the India-ASEAN region.

Shri Shivraj Singh Chouhan stressed on a wide range of aspects involving youth as active participators in building strong and stable relationships among the nations. He stated, "India and ASEAN societies were developed way before the societies of the developed nations developed. Hence our (India-ASEAN) relations have been in existence since time immemorial."

Gen. V. K. Singh spoke of the importance of mutual understanding amongst India- ASEAN nations. He said, "We share values and culture since immemorial times and days are coming when demographic difference will prove to enhance our relationship." He also said, "Youth are the elders for tomorrow, summits and exchanges like this will not only strengthen the ties but will also provide a platform for the cross-cultural exchange of ideas amongst the youth."

Day 2: August 15, 2017

The second day proceedings started with a visit to Manav Sangrahalay. This was followed by a session on India-ASEAN Relations. Ms Preeti Saran, in her keynote address stressed on the recent developments in the relationship between India and ASEAN nations which not only involve improving the connectivity but also about India's attempt to provide financial and technical support to ASEAN. She quoted the role of the youth brigade in strengthening the ties. She also stated that commerce and cultural connectivity has been the hallmark of our relationship and together, we are a perfect example of pluralism in diversity.

Three ASEAN member countries, namely Brunei Darussalam, Cambodia and Indonesia gave their country presentations, in which the polity, culture and tradition of their respective countries and India's relationship with them was highlighted. Parallel discussions took place on four themes: Innovation and Entrepreneurship, Digital and IT connectivity, UN SDGs and Polity and Governance. The sessions were conducted in small groups, and focussed on active participation by the youth, to enlist their views and to facilitate an exchange of ideas.

In the discussion on Polity and Governance, Shri Ram Madhav stated, "We should think beyond democracy, our commitment should be for peace and pluralism and welfare of the last person should be addressed first." The panel discussion on India-ASEAN connectivity was addressed by Dr. Lam Thanh Hah, Senior Lecturer, Faculty of International Economic, Diplomatic Academy of Vietnam; Dr. Vidya Natampally, former Senior Director of Strategy, Microsoft Research India; Dr. Shristi Pukhrem, Senior Research Fellow, India Foundation; and Dr. U. Thein Lwin, Deputy Director General, Dept of Archaeology and National Museum, Myanmar. Dr. Shristi Pukhrem said, "We should join hands to promote connectivity between India and ASEAN since it is very important for cultural and civilisational development." After the conclusion of the day long discussion on various issues, the delegates took part in the ASEAN food festival, where exchange of views took place in an informal environment.

Day 3: August 16, 2017

The 3rd day of India-ASEAN Youth Summit

kicked off with visits to Van Vihar and Bhopal Lake. This was followed by three country presentations, namely Lao PDR, Malaysia and Myanmar. Thereafter, a panel discussion on cultural and civilisational linkages in India-ASEAN region took place, chaired by Prof Sunaina Singh, Vice-Chancellor, Nalanda University. In this Panel Discussion, Dr Ram Niwas, Professor at State Pariyatti Sasana University, Myanmar stated, "Buddhism is the basis of cultural and civilisational linkages and it has also played a significant role in building India- Myanmar relationship." He further added, "It is our common destiny to preserve our cultural and civilisational linkages of India-ASEAN countries since it is a bridge to our future relationship." Cultural and civilisational linkages among countries have always been the basis for any kind of relationship and hence it becomes very important for us to have a comprehensive discussion on it. Shri Sanyal stressed that, "References of cultural and civilisational linkages of a south east region should be given more importance". He further said that the then knowledge epicentre 'Nalanda University' was funded by Indonesian King, Sumatra. Adding to this, Anuradha Shankar, ADG, Administration PHQ, Madhya Pradesh said, "Cultural reality and political reality are not associated and it should not be associated. We have to look at South East Asia from South East Asia's perspective. Everyone has a local and cultural history; resemblances remain, but still differences prevail."

Parallels discussion on the four listed topics were led by Shaurya Doval, Dr Vidya Natampally, Dr Yasmin Ali Haque and Smt Archana Chitnis. The delegation then visited 'Shaurya Smarak' which is a war memorial situated in the heart of Bhopal. From there the delegation proceeded to dinner and cultural event hosted by Shri Shivraj Singh Chouhan, CM of Madhya Pradesh at his official residence. Ms Mithali Raj, Captain, Indian Women's Cricket Team was a special guest for the evening. In her speech, she spoke of the role of women in building up a strong relationship amongst people to make a stable society. She stressed on the importance of youth and urged the youth delegates to work in such a way that they could bring about a positive change in the society

Day 4: August 17, 2017

The day started with a discussion on 'Youth Declaration', where all the delegates had a comprehensive discussion with their respective country members on the draft declaration and some countries came up with their amendment suggestions. Thereafter, the delegates participated in Parallel Discussions, in which different group participated in different discussions. Thereafter, three countries, namely Philippines, Singapore and Thailand gave a presentation of their respective countries. The delegates from Philippines were dressed in their traditional attire that showcased their culture and tradition.

The country presentations were followed by an "Ambassador's Panel Discussion" on Trade and Commerce. Trade and commerce are the backbones of any kind of bilateral relationship since the economies of all countries are inter-dependent. The speakers for this session were Ambassadors of Philippines, Singapore, Thailand and Myanmar. In this session, the Ambassadors presented their trade and commerce data with India. Ambassador of Philippines, H.E Ma.Teresita C. Daza asserted the importance of trade and commerce. She said, "India and Philippines are bonded with trade and commerce and this relationship dates back to the colonial era." Ambassador of Myanmar, H.E U Maung Wai said, "India shares a long border with Myanmar which has the capacity to boost trade and commercial ties between both the countries."

Day 5: August 18, 2017

The last interactive session of the summit was with Members of Parliament on Governance and Policy. This session was chaired by Shri Ram Madhav, Director India Foundation and National General Secretary of BJP. The panel comprised of three Members of Parliament from India, Shri Baijayant 'Jay' Panda, MP Lok Sabha (Odisha), Dr Subhash Chandra, MP, Rajya Sabha (Haryana) and Shri Conrad Sangma, MP, Lok Sabha (Meghalaya). During this interactive session, the speakers asserted the role of youth in politics as a pivotal part of any particular kind of system of government. Shri 'Jay' Panda said, "Political

inheritance gives initial benefit only. Politics is brutal and family linkages have no long term advantage. A vision is required for the service of the Public". Dr Chandra said, "People should not feel neglected since it is the source of any kind of problem." He also said that politics should not start with a wrong mindset and that commitment and endless service to the people is one thing that a true politician should always remember. Conrad Sangma expressed the view that it is never too easy to shape the next step, but faith and ideology are something which will guide you to take the next step. He was of the view that it is very important to maintain a balance between men and women in politics.

Valedictory Session

The Valedictory session was chaired by Shri O. P. Kohli, Hon'ble Governor of Gujarat, with Additional Charge of Madhya Pradesh. Chief Guest for the session was Smt Sushma Swaraj, External Affairs Minister, Government of India. Ms Jayathma Wickramanayake, United Nations Youth Envoy was the Guest of Honour.

Smt Sushma Swaraj said that Ramayana and Buddhism connect ASEAN to India. She spoke of bonds of love and not business and asserted the importance of youth as building each block of a nation. She said, "Youth must debate, discuss and actively participate in shaping discourse on polity, governance and sustainable development agendas". The UN Youth Envoy said that young people need to learn the ways in which humans are able to interact with and adapt to technology and added that in this rapidly changing world, there is no better investment a country can make than in the capacities and potential of youth. Hon'ble Governor of Madhya Pradesh, in his valedictory address spoke of the active participation of youth in various nation building activities, both at national and international level. After this, the Youth Declaration was presented to Smt. Sushma Swaraj.

India-ASEAN Youth Summit not only provided a platform for the young people to have a discussion but also marked the initiation of a forum in which people can come up with views and ideas to address issues of the India-ASEAN region.

◆◆◆

Eighth Round of India-Bangladesh Friendship Dialogue

Shubhrastha

DAY 1: Inaugural Session

Enriching the bilateral ties between India and Bangladesh further, the eighth round of India Bangladesh Friendship Dialogue commenced on 2nd of July in Guwahati. The inaugural event was graced by Md. ShahriarAlam, Hon'ble State Minister for Foreign Affairs, Government of Bangladesh, Shri M.J. Akbar, Minister of State, Ministry of External Affairs, Government of India, Shri Sarbananda Sonowal, Hon'ble Chief Minister of Assam, Capt. Alok Bansal, Director, India Foundation, Shri Dipok Kr. Borthakur, Vice Chairman, State Innovation and Transformation Aayog (SITA) and Dr. Sreeradha Dutta, Director, Maulana Abul Kalam Azad Institue of Indian Studies (MAKAIS), and Shri Pankaj Debnath, Member of National Parliament of Bangladesh. Besides, the event also witnessed the presence of many other esteemed and learned dignitaries.

Shri Borthakur delivered the inaugural speech where he reminded all present of the shared linguistic, cultural and historical heritage and the common troubled past that entwines both nations in an intricate bond. He stressed upon how the river Brahmaputra can open up immense developmental possibilities for trade and commerce, and thereby, bring about prosperity to both nations.

Capt. Alok Bansal threw light upon the significance of the Guwahati Dialogue. He said that this maiden event in NE had its genesis in the idea that such events should not be limited to "mainstream" regions alone, but must be extended to all those regions that share borders with Bangladesh.

Keynote speaker M.J. Akbar discussed the long trajectory of bilateral relations between the two nations. Elucidating upon the slogan of the dialogue - "Brave new world" - a phrase borrowed from Aldous Huxley's novel by the same name, he said that in order to materialise the "New World" envisaged by both the nations, the governments of both the countries are required to have courage; and must work alongside the principles of sovereignty, equality and mutual trust.

Shri Md. Shariar Alam, the other keynote speaker, said that ties between the two nations can be cemented by an equitable share of benefits. He talked about the need to combat terrorism and climate change, and the need for market accessibility in order to achieve collective prosperity.

In his presidential remarks, Shri Sarbanada Sonowal, Chief Minister of Assam focused upon how Prime Minister Modi's Look East Policy for shared growth and prosperity set a benchmark for bilateral relations between nations. He assured that unswerving efforts are being made by the Government to achieve the goals and targets of the policy. Involving students and the youth in such dialogues can boost conflict-resolution and aid policy-making, he claimed.

The vote of thanks was delivered by Shri Pankaj Debnath, Member of the National Parliament of Bangladesh. He asserted that we can grow hand in hand with greater connectivity, sharing of knowledge and expertise, and by establishing diplomatic ties.

This was followed by a short cultural programme wherein performers from both India and Bangladesh put up splendid performances.

DAY 2: First Working Session

Changing World Order and Bangladesh India Relationship

Dr. Sreeradha Dutta shed light on India's bilateral relations and growing political willingness to strengthen them. The land-boundary agreement particularly settled the raw nerves. What Bangladesh has done for terrorism in India is far beyond what we had dreamt of. There have been debates relating to the Rampal Project, environmental issues between the two countries.

The second speaker Manzarul Islam drew upon the hatred, xenophobia, islamophobia being spilled by political leaders. He reflected on how important it is to realise meaning in times of chaos. Energy as well as poverty and maritime security concerns are major issues in Bangladesh. People have largely put it across that they would never prefer any development at the cost of environment.

Prof. Nani Gopal Mahanta put across the burning issues that loom large between the two countries: cross-border terrorism, boundary dispute, illegal border trade, illegal trespassing. Prof. Mahanta recounted the deep roots of culture, history between the two countries.

Journalist Mr. Manjurul Ahson Bulbul expressed how courageous PM Hasina has turned out to be, how she would go to any extent, as long as it concerns the betterment and development of Bangladesh.

Viewing recent relations being affected by internal issues, Capt. Alok Bansal expressed his concern that China's intrusion may affect India-Bangladesh relations. On terrorist activities going beyond national boundaries, he said "Every fundamentalist is a potential terrorist." More

numbers of youth joining the IS is a narrative which demands a counter narrative for resistance.

Second Working Session

Drivers of Mutual Prosperity

The second working session had as its focus area - "Drivers of Mutual Prosperity". Chaired by Ms. Veena Sikri, Former High Commissioner of India in Bangladesh, it sought to focus on issues at the micro and localised levels. Dr. Ainun Nishat of BRAC University Dhaka and Maj. Gen. Dhruv C. Katoch, Director of India Foundation were the lead speakers. The discussants included Prof. Dr. Quazi Kholiquzzaman Ahmed of Dhaka University, Sh. Sabyasachi Dutta, Director of Asian Confluencem, Adv. Mahbub Ali, Member of Parliament, Bangladesh and Dr. Sreeradha Dutta, Director of MAKAIS.

Dr. Ainun Nishat emphasised on the need to introduce joint ventures for enhancing navigational connectivity, water management and hydro-electricity generation. He also asserted that transparency in all government decisions will help build trust and acceptance among people of both the nations.

Maj. Gen. Dhruv C. Katoch focussed on energy-security, cross-border security and the need to build positive narratives and goodwill between the two nations. He said that to combat the various threats disrupting Indo-Bangladesh relations, the defence forces, intelligence agencies and the governments of both the countries should co-operate and act jointly.

Prof. Dr. Qazi Kholiquzzaman Ahmed talked of the ways in which making optimum use of the waterways will open up scopes for earning livelihood for the locals of both the nations. He talked about joint river and basin management and the need to adhere to global standards for arriving at conclusions regarding water sharing in the Teesta river.

Shri Sabyasacchi Dutta highlighted the role of tourism in bringing about growth and prosperity between the two nations. Tourism, he said, will not only bring in revenues but will also generate means of livelihood for the locals of the region and integrate the region. Adv. Mahbub Ali underlined the need to explore new avenues in natural and mineral resources. The easy access of Indian VISA by people of Bangaldesh was also urged upon by Ali.

Dr. Sreeradha Dutta foregrounded the illlegal activities that happen in the transwater boundaries, and the need to come up with effective mechanisms to counter this. She emphasised on developing border-haats so that trade can be carried out legally. She also stressed upon the need for education in the border-area, and the need for combating cattle-smuggling and human trafficking.

Third Working Session

Boosting Connectivity

The third session was focussed on boosting connectivity between the two nations. Shri Pinak Chakrabarty stated that connectivity and security will broadly ensure the development of the North Eastern regions as well as Bangladesh. There should be joint effort to tackle cyber crimes, to explore untapped marine resources and to beat down climatic hazards by focussing on renewable energy.

Dr Moazzem spoke on the economic benefits accrued from the sea ports. He reflected on regional and sub regional projects not getting adequate priority by Indian government. Mr. Shri Kauser Hilaly had spoken about the immense tourism possibilities in Assam targeting the average Bangladeshi tourists.

Dr. Ainun Nishat, another discussant, talked

about how navigation can foster connectivity issues, however, the expenses incurred needs to be addressed. It is feasible only when it is a profitable business. Tarrifs imposed on Bangladeshi goods should be attractive for better transaction so that both nations are benefitted. One can not ignore the financial dimension in regards to railway connectivity.

Ms. Shubhrashtha said that transit routes through Bangladesh can minimise a lot of cost in terms of transportation. Ironically, after decades of independence this type of connectivity is still new. Stressing on the need to solve security and development issues simultaneously because they are not antagonistic in nature, she also shed light on the linking of textile and fabric industries of Bangladesh and North East. She articulated that connectivity between the two nations should be taken with renewed focus.

The next speaker Dr. Delwar Hossain spoke of connectivity as an instrument of development and also a discourse. He pinpointed how to integrate the whole South Asian region with connectivity.

DAY 3: Fourth Working Session

Mechanism for Sustenance of Good Relationship

This session had "Designing Long-Term and Forward Looking Mechanisms for Sustenance of Good Relationships" as its focus.

Dr. Qazi Kholiquzzaman Ahmed urged multinational companies of India to also target Bangladesh for their investments. This, he said, will boost the economy and generate employment. He also focussed on the responsibility of Internal Security Forces in combating transborder smuggling.

Shri Tarun Vijay talked about the concept of 'Ashta Padma' - the eight milestones that will bind people of both nations. He also talked about how

a brave and secular spirit will help the sustenance of good relationships. Vijay discussed how a prosperous future can be shared by both nations through developing education, connectivity, healthcare and the security forces.

Dr. K.K. Dwivedi narrated how investments and turnovers have seen a boost over the past year and how the export-import trade between both the nations have helped both economies to grow. He also talked about the need for developing dredging mechanisms, transit facilities and business opportunities.

Shri Moazzam Ali talked of the need to develop knowledge based societies and people-to-people relationships. He also stressed upon developing borderline economic zones.

Shri R.P. Sharma focussed on the importance of border management, good transport and communication system and the inclusion of students in shaping amicable Indo-Bangladesh relations.

Shri Shishir Shil talked about the need to include the history of 1971 War for Liberation and India's contribution in it in the academic syllabi of both countries. This, he said, will help build goodwill. He focussed on the need to build a Joint Education Task Force.

Shri Binod Bawri said that for long-term and forward looking mechanisms for sustenance of good relationships, we need to bring about increase in trade and commerce, travel, tourism and technology.

Valedictory Session

The Valedictory Session was chaired by His Excellency Shri Tathagata Roy, Honourable Governor, State of Tripura. The keynote address was delivered by Shri Shahriar Alam, Hon'ble State Minister for Foreign Affairs, Government of Bangladesh, who shared his wonderful experience during the last two days in the city of Guwahati before the august audience. He spoke on how the different issues like Changing World Order and Bangladesh India Relationship, Drivers of Mutual Prosperity, Boosting Connectivity, Designing Long Term and Forward looking mechanisms for sustenance of good relationship occupied the esteemed speakers and discussants. He said that there is no doubt in the fact that India Bangladesh ties are not only long-lasting and time-tested, but there is also a huge possibility of increasing people-to-people contact between the two nations. Though India Bangladesh friendship ties under the dynamic leadership of Prime Minister Narendra Modi and Prime Minister Sheikh Hasina are at an all time high, he stressed the need to remove the different irritants like terrorism and poverty plaguing the two nations. He reminded everyone how the triangle comprising Bangladesh, Nepal, Bhutan and North East fall under the poorest regions of the world that can be overcome with shared resources, expertise and boosting connectivity through regional and continental highways, rail networks, seaports and coastal shipping. Further he added that there is a huge aspiration for peace and collective prosperity and the partnership between India and Bangladesh based on trust and sovereignty can set a benchmark for the rest of the world to emulate.

Shri Ram Madhav, National General Secretary, BJP and Director, India Foundation elucidated the noble vision of Prime Minister Modi "Sabka Saath, Sabka Vikas" where the latter considers Bangladesh as a true partner in the development of the East. He articulated that the cow is sacred to the Indians but life is more sacred to them and

he condemns the lynching of people by the so called cow savers. He expressed the hope that just like the people of India expect to see Narendra Modi for many many years after 2019 rendering his service to the nation, the people of Bangladesh too would like to see Prime Minister Sheikh Hasina for many many years in the service of the nation. He dwelt at length how Sheikh Mujibur Rahman envisioned Bangladesh as a secular nation state and his efficient daughter Prime Minister Sheikh Hasina is carrying out his dream in the best possible manner. While referring to the issue of illegal movement of cattle across the border from India to Bangladesh, he stressed the need to devise means to check such activities. He also referred to issues of religion and religious fundamentalism that the two neighbouring nations are to deal with a strong hand. He reflected that though India and Bangladesh have reached common ground so far as combating terrorism and trade and commerce are concerned, but issues like water sharing need to be dealt with. He assured that government of India is committed to fulfil the assurances given by previous governments. Acknowledging the fact that both nations face certain external and internal challenges, he hoped that it shouldn't deter the two nations to deviate from their cherished values like democracy, secularism and love for peace while confronting challenges like terrorism and religious fundamentalism that will ensure the two neighbours to move forward together. He hoped that under the leadership of Prime Minister Modi and Prime Minister Hasina, the two nations will scale new heights of progress in the field of education, health and commerce and further consolidate their bilateral ties.

In the valedictory address by Shri Himanta Biswa Sarmah, Minister of Finance, Government of Assam, the august gathering was reminded of the different issues discussed in the dialogue process and expressed his gratitude at organising the event in the city of Guwahati. He said that he would be failing in his duty if he doesn't mention how the people of Assam feel about the problem of illegal immigrants from Bangladesh. He further added that with the completion of National Register of Citizens, those illegal immigrants would be identified and the issue will be taken up by the

Government of India, with the Government of Bangladesh for an amiable solution. He expressed his gratitude towards Hasina Government for uprooting the bases of different insurgent groups like ULFA and thus contributing to peace and tranquillity of the North Eastern states. The Minister said that the north-eastern states and Bangladesh can join hands to create world class institutions and facilities in the areas of education and health care. He further added that transit of goods to the Northeast from other parts of India through Bangladesh can benefit Dhaka not only by means of earning transit fee but it will also improve the service sector in Bangladesh. It will also serve the cause of Northeast as it will cut down the expenses of transportation.

In his enlightening Presidential remarks, Shri Tathagata Roy, Honorable Governor, State of Tripura, remarked that Bangladesh is one nation that was created on the bedrock of its linguistic identity. He spoke at length how Bangladesh and India not only share the same culture, values and civilisation but even the National Anthem of the two nations were composed by the same literary genius which is not a small deal. He recollected one of the highly attended assemblies in the Brigade Parade Ground, Kolkata in the year 1972 where Sheikh Mujibur Rahman made his historic speech where he envisioned Bangladesh as a secular country where people of all religions can freely practice their religious beliefs. He regretted how religious fundamentalism and extremism tried to mar his dream by demolition of Hindu temples and offering resistance to celebration of Hindu festivals though under the leadership of Rahman's daughter Sheikh Hasina the minorities are now feeling safe and their interests protected.

He expressed his personal opinion that as per international law all lower riparian states are entitled to have their share of water and India cannot deny water to Bangladesh. He was very vocal in the expression of his opinion that if India feels that sharing of water will lead to shortage of water in India, then even the shortage can be shared. He stressed upon the need of sharing water not only of Teesta but also of other rivers that flow to Bangladesh. He expressed his fears that if China constructs dams in the Siang river, it will not only be detrimental to India, but it will also affect Bangladesh.

He spoke on the relationship between Kazi Nazrul Islam and Shyama Prasad Mookherjee which forms the bedrock to understand the relationship between India and Bangladesh. Recounting episodes of genocide by Pakistani Army, he stressed on the need to keep the fundamentalist forces at bay. In his enriching speech, he tried to map the different rivers that flow from India to Bangladesh and deliberated how the two nations can benefit through water sharing and ensuring better connectivity. He discussed at length the literary works of different writers like Syed Mujtaba Ali who knew fifteen languages to Kazi Nazrul Islam. He acknowledged that the government of Bangladesh has done more than India can expect to ensure that the country is not used as a sanctuary by militant outfits like ULFA as such insurgent groups have been hounded out from Bangladesh; however some Bangladeshi extremists have found sanctuary in India. He also urged that granting of medical visas to Bangladeshi nationals should be done on an urgent basis to ensure better friendship ties.

◆◆◆

India Foundation Dialogue on
The Future of India-UK Relations – British Elections, Brexit & Beyond

Apoorva Goel

India Foundation organised the 38th India Foundation Dialogue on 4th July, 2017 at India Habitat Centre, New Delhi. The session was themed 'The Future of India-UK Relations - British Elections, Brexit & Beyond'. The dialogue was a panel discussion with Lord Jitesh Gadhia, Shri Ranjan Mathai, Shri Asoke Mukerji and Shri Ashok Malik and was chaired by Shri Jayant Sinha, Minister of State for Civil Aviation, Government of India and witnessed an audience of more than fifty people.

"There comes a tide in the affairs of men, which taken at the flood, leads on to fortune. On such a full sea are we now afloat and we must take the current while it serves, or lose our ventures. That is the opportunity that confronts us today when we talk of India and UK," said Shri Jayant Sinha in his opening address. He said that it was extraordinary that India and UK, though furthest apart geographically, are closest culturally. He stated that India can forge a partnership with UK in multiple sectors that can be quite defining globally, particularly focusing on finance, technology, science and innovation, and mass services. "In finance", he said, "we have moved forward in interesting ways, an example being masala bonds, used to finance large aspects of infrastructure and other industries, which was initially thought to be very difficult to implement in India." These masala bonds are important for India since we need debt financing, and they also strengthen London's position by working with an emerging country. Talking about science, technology and innovation, he said that UK has a cutting edge in technology, with fast development in even Artificial Intelligence. And because of our large IT and BPO sectors, we need that kind of expertise. As UK looks for areas where it can

invest and develop other than in the European Union, science, technology and innovation becomes another area for us to really start forth some unique bonds. Coming to mass services, he said that by taking software and AI expertise, we can make mass services like financial inclusion, mass entertainment much more affordable, cheaper and effective. So, expertise coming through UK and being applied in India is the basis on which we (India) can become an entrepreneurial engine for next 60 billion people.

Shri Ranjan Mathai suggested that what we need to do is to take those elements that make a winning partnership and build on them, economic opportunities being the first of them. He said that London is able to mediate, absorb funds from all around the world and then direct them to places where serious analysts can utilise them. He then addressed the issues of national security, terrorism and cyber security. He also said that today we are in an age of populism, nationalism where ideologies differ. But the fact that both the nations are democracies matter a great deal. In conclusion, he said that UK is a country that has changed the most in changing its perceptions towards immigrants but now it has reached a point beyond which it cannot go on indefinitely and we need to respect that and learn to manage our demands from UK. On Britain's side, they must ensure that Indian people are not discriminated in any way there.

Lord Jitesh Gadhia began by thanking India for its continued friendship with UK and being a source of fresh thinking and ideas to be discussed. On the financial front, he agreed with other speakers regarding the win-win partnership. The question that according to him needs to be paid attention to is, 'What will happen to London after Brexit? Will it retain its pre-eminent position?' He further explained that London has 250 foreign banks operating, more than at any other centre. These banks account for 40% of world's foreign transactions. "There is no room for complacency and there is some serious architecture to be developed around London's position."

Shri Asoke Mukerji said that the first reality that we have to understand is that global multilateral system, which was created by UK,

USA, Soviet Union, China, and France in 1945 is not going away. Irrespective of a soft or a hard Brexit, UK has a weight as a permanent member of the United Nations Security Council. For winning the partnership with UK, he focused on four political areas. The first being the use of diplomacy for peace, which he believed can be done by giving an opportunity to a country like India- an Asian country that has never been given such an opportunity since the end of the Cold War. The second area was to make UN peace-keeping more effective as there can be no development without peace. The third was to make India a permanent member of UNSC so that India can also be a decision-maker. The last area was countering terrorism, which is the single biggest challenge to international security. He concluded with the issue of technology, saying that in UN, India has been among the few nations from developing countries to call focus for innovation, incubation and transfer of technology for development. "Focus on technology will play an important role in multilateral aspect of a win-win partnership," he said.

In his address, Mr. Ashok Malik said that when Britain looks at India today, it needs to understand where it stands in India's foreign policy because this is a newer, more pragmatic, more transactional India. But, according to him, Britain has, at this point, sent conflicting signals. There are two Britains - one which says that this is a moment for Britain to make the best of its partnership with India for both sides, and the other one which is talking about becoming European Singapore. He said that India is clear on which one it wants to talk to, but Britain needs to take a decision. "The potential for an India-UK economic relationship is actually agnostic to any friendship. There is a natural synergy between Britain's technology and Make in India, between India's modernisation and British innovation." He also mentioned two challenges - market access and agreement on details of international security - in the India UK partnership.

◆◆◆

REPORT

Fudan-India Foundation
4th Annual Bilateral Dialogue at Shanghai

Siddharth Singh

India Foundation Delegation undertook an academic visit to China from 11th to 16th July, 2017 as a part of the 4th round of Fudan University - India Foundation Dialogue on the theme "India-China Relations in Transition". Capt Alok Bansal, Director, India Foundation led the India Foundation delegation while Prof Zhang Jiadong, Director for South Asian Studies, Fudan University led the Chinese side. At Kunming, Prof. Zhu Cuiping of Research Institute of Indian Ocean Economies at Yunnan University of Finance & Economics steered the deliberations. The other members of the India Foundation Delegation were Shri Shakti Sinha, Director, Nehru Memorial Museum & Library, New Delhi; Shri P. Stobdan, Senior Fellow, IDSA & former ambassador; Shri Prafulla Ketkar, Editor, Organiser; Prof. Nani Mahanta, Gauhati University; Dr. Shristi Pukhrem Senior Research Fellow, India Foundation and Siddharth Singh, Research Fellow, India Foundation.

During the visit, India Foundation delegation interacted with academics & scholars of Fudan University. The interaction witnessed scholarly and candid exchange of views from both sides on critical issues such as Sino-India relations in the changing international system, cooperation & competition between India and China in South Asia & Southeast Asia, Sino-India cooperation in multilateral forums, Doklam stand-off and

prospective solutions to the way forward for relations between two countries.

Inaugural Session

Prof. Zhang Jiadong, Director of Center for South Asian Studies, IIS, Fudan University, chaired the inaugural session and welcomed all the delegates. In his inaugural address Professor Wu Xinbo, Executive Dean of Institute of International Studies, Fudan University highlighted three issues which are important for China in 2017- a) 19th National Congress of the Communist Party of China, b) Belt & Road Initiative of China, c) Innovation, Green Development & Progress. Prof. Wu Xinbo also suggested that "to better manage disputes and differences, it is now imperative to build trust between Beijing and New Delhi. The foreign policy and strategic circles of the two countries need to maintain dialogues and communications on a regular basis. Equally important, people-to-people exchanges are indispensable to consolidate better understanding of the will of the people of the two countries."

Capt. Alok Bansal, Director, India Foundation, in his Special Address emphasised the importance of furthering bilateral relations and consolidating the developmental partnership, which was established during the visit of Chinese President Mr. Xi Jinping to India in September 2014 and subsequently during the visit of Prime Minister Shri Narendra Modi to China in May 2015. He also highlighted the cooperation between India and China in various multilateral frameworks like AIIB, G-20 and BRICS. On the Doklam stand-off, Capt. Bansal put across the Indian point of view and the apprehensions on the issue in unambiguous terms. He also highlighted that it is essential for all concerned parties to display utmost restraint and abide by their respective bilateral understandings and not to change the status quo unilaterally. Capt. Bansal also raised the issue of terrorism and said that India and China cannot afford to have

differences on terrorism. He raised the need to designate Jaish-e-Mohammad Chief Masood Azhar as a terrorist at the U.N. on which all other countries except China and Pakistan have agreed.

The Keynote address was delivered by Major General ZHU Chenghu (Retd). His address mainly focused on recent Doklam stand-off between India and China on the border. He alleged that "the Indian border troops crossed the China-India boundary at the Sikkim section and entered the Chinese territory and had obstructed Chinese border troops' activities in Doklam. Maj Gen Zhu refereed to the treaty of 1890 in which the Sikkim section of the China-India boundary was defined by the Convention between Great Britain and China relating to Sikkim and Tibet. In his final remarks, Major Gen Zhu suggested that Indian side should follow the boundary convention as per treaty of 1890, respect the China's territorial sovereignty and thus Indian troops should immediately withdraw from the disputed border to safeguard peace and tranquillity.

Session-I

This session focussed on "Sino-India Relations in the changing International System". Capt. Alok Bansal started the deliberation by talking about the setback to the globalisation. To him, the difference that exists today between India and China is a dispute. In the larger context, there are two biggest threats to both the countries and the world - climate change and terrorism. With regard to terrorism, it is the threat from non-state actors. For every act of terrorism there is a theological narrative. In the light of this, India and China should evolve a common strategy to counter this threat.

Shri Shakti Sinha said that tranquillity along the India-China border was an important

prerequisite for a peaceful relationship with China against the backdrop of a tense military standoff between countries on the Doklam plateau in the Sikkim sector. He highlighted that Beijing's external aggression is also an outcome of its increasingly nationalistic domestic politics under President Xi, who is heading into an important Party Congress in November. Shri Sinha underlined that so far India has been mature in its approach to the stand-off, providing no provocation to the Chinese by any military movement or through its official statements. He said that the dispute in Doklam area is not a new phenomenon. He emphasised that China's road construction in Doklam is a deliberate move to trigger a response from Bhutan and from India. Through its actions, China seeks to impose its own definition of the tri-junction point of the boundary between Bhutan, China and India (Sikkim). The move has serious security ramifications for both Bhutan and India's defence interests.

Prof. LONG Xingchun flagged the importance of issues related to the Indian Ocean. He also mentioned about the current border disputes (Doklam incident) and condemned it. Prof. Xingchun especially pointed out the statement given by the Indian defense minister who said that the response from the Indian side will no longer be similar to that of 1962 conflict.

Amb. P. Stobdan took off the discussion by talking about how the world is changing since the last six to seven months. He specifically mentioned regarding how the European Union (EU) taking a confrontationist line with the United States (US). According to him, climate change and international trade have become two of the most important features of the international system. Further, the situation in the Middle East cannot be ignored. On

India-China relations, he said that the changes have come because of structural differences. The foundation of India-China relations is missing today. In order to strengthen the ties, there is a need to build relations on strategic trust. Citing the examples of Bollywood movies, namely 3 Idiots and Dangal which are very popular in China, he said cinema could be used as a medium to develop further ties between the two countries. Talking on the Belt and Road Initiative (BRI), India is an infrastructure investment part of the AIIB. He said BRI should respect the territorial integrity of India. Responding to the Chinese delegation's concerns, Amb. Stobdan clarified that India-US relations should not be considered as a constraining factor in India-china ties. He summed up by expressing India's firm stand to continue maintaining the status quo with regard to the Doklam incident.

In his remarks, Prof. Guo Xuetang said that the current stalemate between India and china is a period of trust deficit. He also talked about PM Narendra Modi's foreign policy, and the importance the Indian government gives to neighbourhood policy and "extended neighbourhood". Alongside this, PM Modi's economic policy and efforts to improve living standard was highlighted by the speaker. Dr. Huang Yinghong pointed out the weakness in India-China economic and cultural relations. These two factors remain too weak to improve the overall ties. However, he did not rule out the potentials and benefits of economic cooperation. He concluded by saying that both countries should maintain the strategic and security compatibilities which are necessary.

Prof. Hu Zhiyong talked about cooperation and confrontation between India and China in Southeast Asia. He also mentioned about how Southeast China connects India and the Pacific. On political arena, he spoke of India's role in the ASEAN Regional Forum (ARF), and also the emphasis given by New Delhi on Act East Policy. The differences in trade ties between India and ASEAN and China and a few of the ASEAN countries were also highlighted by him. Lack of connectivity between India and ASEAN, according to the speaker, is the biggest obstacle. India's increasing role in the South China Sea has been considered by him as a factor for the competition between India and China in this region. In concluding remarks, he identified areas of cooperation between India, China and ASEAN: 1) Build mutual political trust, 2) Increase more contacts, 3) Develop the triangular friendly partners among China, India and the ASEAN countries, and, 4) Close the gaps between these countries.

Section-II

This session was devoted to "Cooperation and Competition between China and India in South Asia and Southeast Asia". The following was discussed:

- The internal or the domestic factors should not be ignored while discussing India-China bilateral relations.
- Strategic differences should be managed.
- Relations should not only be looked from the prisms of geopolitics or geo-economics but also from the geo-civilisational paradigm.
- There is a requirement that the Asian parameter (India and China) should not be studied only on ideological terms but from the strategic perspectives of both Confucianism and Hinduism.

Both sides of the delegation discussed how to cooperate more and compete less. There was also a view that ASEAN could be a common platform where India and China could cooperate. Notwithstanding the significant role China is already playing with some of the ASEAN countries, India should also strive further to engage more constructively with these countries, in line with the present Indian government's Act East Policy. The concept of Indo-Pacific was adequately discussed and some even highlighted the role of India and China as prominent players. In this regard, their cooperation and competition in the Indo-Pacific region were flagged.

Session-III

In this session the conference discussed "CPEC and Sino-India relations". Indian delegates made it clear to Chinese side that connectivity projects must be pursued in a manner that respects sovereignty and territorial integrity. Since China as a country is very sensitive to its own sovereignty, it must also show the same sensitivity when it comes to India. Indian delegates also made it clear that "Connectivity initiatives must be based on universally recognised international norms, rule of law, openness, transparency and equality. Connectivity initiatives must follow principles of financial responsibility to avoid projects that would create unsustainable debt burden for communities; balanced ecological and environmental protection and preservation standards; transparent assessment of project costs; and skill and technology transfer to help long term running and maintenance of the assets created by local communities. Any connectivity projects in the territory which is constitutionally a part of India and not part of Pakistan must be pursued in a manner that respects sovereignty and territorial integrity of India."

Shri Shakti Sinha, in his presentation, mentioned that China's aggressive pushing of its One Belt One Road (OBOR) initiative, particularly in the countries in India's neighbourhood has created substantial disquiet as it has domestic (as in host country) political implications. The China Pakistan Economic Corridor (CPEC) would pass over territory that is legitimately India's but in unlawful occupation of Pakistan; a departure from China's stand at multilateral financial institutions where it objects to any project in any territory over which it lays claim.

Session-IV

This session focussed on "Sino-India Cooperation in International Multilateral Arena". The discussion was embedded in optimism about the broad changes in the international relations paradigm, but a cautious optimism that took into account the various aberrations that stand in the way of global security and stability. Ultimately, as was noted, geopolitical rivalries have existed for over a long period of time in the world politics and will continue, but what is at stake is how countries like India and China adjust the relativities in the changing global order and agreed that the international situation is in flux and both India and China have been beneficiaries of a stable and open international system and at this time probably one thing that both countries could do together was a more stable, substantive, forward looking India-China relationship which would inject a greater

amount of predictability into the international system. Indian delegates highlighted that future progress in strategic cooperation between China and India in the changing international order in the next decade or beyond will be determined by the will, and more importantly, concerted efforts of the two countries. Indian leadership is devoted to developing healthy and stable China-India relations on the basis of equality and mutual benefit, enriching strategic cooperation and expanding the convergence of interests. Such commitment is required from both sides if the two countries are to avoid the tragedy of the rise of other major powers, break the shackles of geopolitical calculation and jointly shape a future of mutual benefit and common prosperity.

The delegation of India Foundation also visited Shanghai Academy of Social Sciences in Shanghai and Research Institute of Indian Ocean Economies at Yunnan University of Finance & Economics in Kunming. At both the places, during the discussions, delegates from both sides discussed a wide canvass of issues affecting India and China relations including the ongoing border standoff in Doklam area. The Chinese delegates raised the current issue of Doklam stand-off in their presentation. The Indian delegates put across the Indian point of view and the apprehensions on the issue on our side.

Apart from the Doklam stand-off, discussions were mainly held on the issues of India-China relations in the changing international system, cooperation and competition between China and India in South Asia & Southeast Asia, the China-Pakistan Economic Corridor and India-China cooperation in international multilateral arena. The discussions were held in an amicable atmosphere and the delegation put across points related to the politico, economic, cultural and security aspects pertaining to India-China relations. Both India and China have a long civilisational legacy and no third actor should determine the bilateral ties, was the general sentiment on both the sides. The need to address and respect each other concerns both on sovereignty and maritime front was also underscored. Both sides expressed their desire of bettering ties between the two countries because improved relations between two countries are in the interest of both India and China and of the global community.

◆◆◆

Young Thinkers Meet 2017

Ngawang Hardy

Young Thinkers Meet is a flagship India Foundation event. It is a two day conclave of young intellectuals who brainstorm over various issues of national significance. The 6th Young Thinkers Meet (YTM) was organised by India Foundation on 30-31 July 2017 in Vadodara, Gujarat. The meet, themed **'India 2047'**, was well attended by dignitaries and over 70 young intellectuals from diverse educational and cultural backgrounds. Varied themes were covered during the course of the meet.

Shri Swapan Dasgupta, Member of Parliament (Rajya Sabha) and Shri Ram Madhav, National General Secretary, BJP and Director, India Foundation, welcomed the participants in the inaugural session. Shri Ram Madhav explained the purpose of the meet. He said purpose of YTM is to define an innovative, developed India, an India we perceive in 2047 and roadmaps for building that India. Shri Swapan Dasgupta remarked that in India, we used to worship knowledge. In the west, they worshipped power. But knowledge combined with power becomes an undefeatable force. We have to break out for a 'New India' and continue the process of unlearning and relearning.

Inaugural session was followed by a session on 'Financial Empowerment and Economy in Transformed India'. Shri Shaurya Doval, Director, India Foundation & Shri Saket Misra, CEO, Venus Asset Finance led this session. Issues related to

the trend of rising population, financial inclusion, financial independence, job opportunities, questioning and re-defining 'work' etc. were discussed in this session. The speakers mentioned that the key to progress are the three Ds - Demography, Digitisation and Dynamism. Speakers mentioned that there is a need for creating a cooperation economy through '*sarvodaya*' and '*antyodaya*'.

Shri Shakti Sinha, Director, Nehru Memorial Museum and Library led the session on 'Public Institutions in Transformed India'. He described the state and nature of Public Institutions in India and stressed the need for critical thinking in Public Institutions. He talked of decentralisation and strengthening local governance. This was followed by a session on 'Transforming Democracy in India', led by Shri Ram Madhav. He said that the best way to ensure transparency is to disincentivise electoral politics.

Other sessions during the meet were on 'Role of RSS and other social movements in Transformed India' and 'Education and Dharma in Transformed India'. These were led by Swamini Vimalananda, Acharya, Chinmaya Mission and Shri CR Mukunda, Sah-Baudhik Pramukh, RSS. Shri CR Mukunda threw light on the role and objectives of RSS in transformed India and the challenges it faces. He shared some of the RSS objectives and initiatives like *Samaj Parivarthan* (transformation of society), *Vyavasta Parivarthan* (transformation of system), *Sajjan Shakthi Jagaran* (awakening of the good) etc. Swamini Vimalananda began her session by stressing on the need to question. She said to transform we have to break out of the American's old lifestyle that we are today living. We need to come out with our own Unique Selling Point (USP). She described learning by way of tuition and intuition. Swamini said Indian way has respected both the ways equally and laid stress on value education.

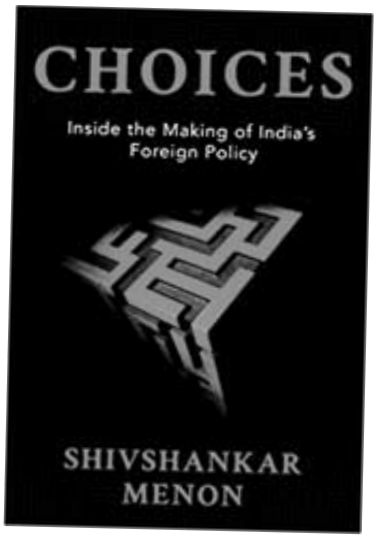
The Young Thinkers Meet saw two new initiatives this year - one panel discussion and the other Mock Parliament. The discussion on 'Media in Transformed India' saw participation of Prafulla Ketkar, Editor, Organiser; Kushan Mitra, Managing Editor, The Pioneer; Prashant Jha, Associate Editor, Hindustan Times; Rumu Banerjee, Assistant Editor at Bennett Coleman and Co. Ltd. and Smriti Kak, Journalist, Hindustan Times and the Mock Parliament saw participants discussing issue of 'Beef Ban' and 'Demone-tisation'.

Participants at the Young Thinkers Meet made presentations around the theme 'India 2047', shared their initiatives, participated in the 'India Quiz' and discussed interesting books.

The valedictory session was presided over by Shri Ram Madhav and Shri CR Mukunda. Shri CR Mukunda said that transformation is not possible without thinking of the last (wo)man standing. He encouraged participants to work at the grassroots. Shri Ram Madhav, asked participants to be confident in one's thought. He reminded all delegates that it was important to co-opt rather than confront those who might disagree with us. He urged delegates to be 'respectful', be 'magnificent' but at the same time have the 'killer instinct' and win the argument.

◆◆◆

Choices
Inside the Making of India's Foreign Policy



Author: **Shivshankar Menon**

Publisher : **Penguin Random House India, 2016, pp 224**

Price: Rs.599/-

Book Review by: **Jerin Jose**

"Strategy consists of making the most of available means to achieve one's goals. India's goal is to transform India"
- Shiv Shankar Menon, Choices

India's former National Security Advisor (NSA), Shiv Shankar Menon's book "Choices: Inside the making of India's Foreign policy" is a good read to understand the post-cold war decision making in Indian foreign policy. Mr. Menon describes the insider's account of five crucial scenarios India has faced during his long career in government. The border peace and tranquility agreement with China, the negotiation of the nuclear agreement with the USA, India's response to the 26/11 Mumbai attacks by Pakistani terrorists, the final stages of Sri Lankan civil war and the evolution of India's nuclear doctrine -'No First Use policy'. In each case, Menon starts with the context, the choices that Delhi had to make and the lessons from these decisions. He also clearly explains the intricacies of getting things done within the political and institutional constraints that he faced which remind us about the need for reforms in India's governance structures. Menon's clear articulation of complex topics and command over the details makes each account a very exciting and informative read for anyone interested in India's foreign policy.

He starts with the 1993 Border Peace and Tranquility Agreement with China – the first ever boundary related agreement between modern states of India and China in which he played a crucial role. He dwells deeper into the historical aspects of India-China 'border', the 1962 war, Chinese strategy regarding India and Pakistan and its greater goal of becoming a preeminent global power, the intricate details of the negotiations and the calculations which went into the making of the agreement and finally the lessons learned from the agreement. Menon is of full praise to former Prime Minister P.V. Narasimha Rao for leading public opinion and building consensus while bringing along his political opponents for the fruition of the agreement.

The second chapter deals with the Civil Nuclear initiative between India and USA which was started by the first UPA government and which became the pillar of trust and cooperation between

**Jerin Jose is a Young India fellow, from the 2016-17 batch at Ashoka University. He can be reached at jerinjose1906@gmail.com*

India and USA. He covers the entire negotiations which happened between India and USA as well as in international agencies like IAEA, Nuclear Suppliers Group as well as in the US Congress and Indian Parliament. He concludes the chapter by explaining what the civil nuclear initiative means for the larger geopolitics in the 21st century. In his own words the Indo-US nuclear agreement was always much more than a dollar and cents calculation or the import of reactors, or cheap renewable energy for India's future. It was about much bigger things - like the strategic need to stand up together to balance the rise of China and chart a new century of cooperation between two countries whose strategic objectives converge almost on every aspect in Asia.

The third chapter deals with the question of why India didn't use overt force against terrorist groups based in Pakistan after the 26/11 attacks in Mumbai in 2008. After dissecting the decision to not militarily respond to the 26/11 attack on Mumbai, Menon argues Prime Minister Manmohan Singh made the right decision not to respond. But at the same time, he believes that future Indian governments will not be so restrained as the context and personalities heading the country has changed.

India's involvement in the Sri Lankan civil war is one of its most traumatic overseas adventure till date. It led to thousands of Indian deaths including that of the former Prime Minister Rajiv Gandhi. Chapter four deals with India's experience in Sri Lanka during the Sri Lankan civil war and how choices were made by New Delhi by giving the detailed overview of the different interests and strategic calculations which went into each decision.

Chapter five deals with India's nuclear doctrine of 'No First Use' and he explains clearly why this is the best policy for India which allows India to focus on domestic transformation and economic growth without wasting time and effort on a nuclear arms race. But at the same time and gaining a strategic equivalence by indulging in deterrence strategy.

Menon concludes the book with a valuable reflection on India's international destiny, its strategic culture and the kind of great power it might become. He offers insights into the emerging constraints on statecraft in this century and the need for strong institutional mechanism to solve issues in the foreign and security policymaking in the coming decades. Menon doesn't answer directly to the question of whether India has a strategic culture but affirms that there is an Indian way of foreign policy which is "marked by a combination of boldness in conception and caution in implementation, by the dominant and determining role of the Prime Minister". Menon warns Delhi against embracing ambitions of becoming a traditional great power and forgetting the priority of domestic transformation and reminds of Germany and Japan as examples of rising powers that prematurely thought that their time had come for global domination. Menon ends the book with the discussion on why India needs to be a great power and how it should be a 'different power' which uses its power first for domestic transformation of India itself.

Choices should be considered as one of the rare good books on the inside deliberations and thought processes which go into making the Indian security and foreign policy decisions. It is a must-read for anyone who would like to know how and why India has made certain 'choices' in its relations with the outside world and how it is trying to be a great power with a difference.

◆◆◆

Upcoming Events

Workshop on Jihadi Terrorism in the Af-Pak Region and its Regional Implications

11-14 Sept, 2017; Herzliya, Israel

India Foundation will be hosting a workshop on **Jihadi Terrorism in the Af-Pak Region and its Regional Implications** at the International Institute for Counter-Terrorism (ICT)'s World Summit on Counter-Terrorism 2017. The workshop will cover following issues:

1. Causes of Radicalization in the region, factors contributing to the growth of IS & Taliban.
2. Linkages between Al Qaeda, Taliban, IS and other radical Islamic organisations.
3. Inter-dependence of these organizations to meet the theological requirements of 'jihad'.
4. Pakistan's tacit support to Taliban and its impact on international attempts to fight it.
5. Implications of growth of jihadi outfits on the region at large and on India in particular.

Conference on 'Smart Border Management'

18-19 September, 2017; New Delhi

India shares 15,106.7 kms of its boundary with seven nations - Pakistan, China, Nepal, Bhutan, Myanmar, Bangladesh and Afghanistan. These land borders run through different terrains, and managing a diverse land border is a complex task but very significant from the view of national security. In addition, India has a coastal boundary of 7,516.6 kms, which includes 5,422.6 kms of coastline in the mainland and 2,094 kms of coastline bordering the islands. The coastline touches 9 states and 2 union territories. Indian Navy and Coast Guard are vested with the responsibility of coastal borders, where the State Marine Police is acting as the second line of defence.

The 2nd edition of the conference 'Smart Border Management', which is jointly hosted by India Foundation and FICCI, aims to address the emerging challenges faced by India post Uri attack in smart border management, by bringing national and international stakeholders together to discuss how India can create smart borders that, on the one hand, allow enhanced trans-border movement of people, goods and ideas, and on the other, minimise potential for cross-border security challenges.

For further details, please write to **mail@indiafoundation.in**

Conference on UNCLOS

4-6 October, 2017

Port Blair, Andaman & Nicobar Islands, India

United Nations Convention on the Law of the Sea (UNCLOS), also referred to as the "Constitution of the Oceans", is a detailed instrument that covers a wide range of issues of governance of ocean spaces and the resources therein.

UNCLOS solutions for managing the global ocean common will be the underlying theme of the Conference. Delegate participation from various countries have been invited to discuss the following:

- Enduring legitimacy of UNCLOS & its continuing vitality in 21st century
- Role of UNCLOS in facilitating peaceful settlements of disputes: A case of harmonious maritime dispute resolution-India, Bangladesh & Myanmar
- Growing problems of non-compliance with UNCLOS: Analysing imbroglio in South China Sea
- Maritime Security architecture in the Indo-Pacific region to maintain freedom of navigation under UNCLOS

For further details, please write to **mail@indiafoundation.in**

International Conference on "BIMSTEC: An Enabling Architecture for Growth, Prosperity & Partnerships"

4 - 6 November, 2017; Guwahati

The seven member states of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) provide unique links between South Asia and Southeast Asia. The region is home to around 1.5 billion people (22% of the global population) with a combined GDP of US$2.7 trillion. In the last 5 years, BIMSTEC members states have been growing at 6.5% on an average. It is also a large consumer market despite global economic slowdown. Now as their shares in global trade, economy and growth are rising, the sub-region is fast becoming geo-economically significant for global powers. BIMSTEC is also of utmost geostrategic and economic importance for India.

It is in this backdrop that India Foundation in partnership with FICCI, will be organising a BIMSTEC Conference for the generation of debate, discussion and the exchange of ideas on the sub-grouping and its future development. In other words, it would be a track 1.2 dialogue to streamline the future course of BIMSTEC. The conference would provide inputs based on a comprehensive understanding, for charting out the future course of BIMSTEC in the medium and long run and recommend, if required, the necessary improvements in the existing mechanisms. The conference will consist of eminent personalities/stakeholders of diverse background (from the government, academia, think tanks, civil society and the media) including from all BIMSTEC member states.

For further details, please visit **www.bimstecconference.in**

4th International Dharma Dhamma Conference

30 Nov – 02 Dec, 2017; Rajgir, Bihar

Centre for Study of Religion & Society, (CSRS), India Foundation in collaboration with Nalanda University, Rajgir is organizing 4th International Dharma Dhamma Conference on the theme "State and Social Order in Dharma Dhamma Traditions". The conference seeks to explore the shared values of the dharmic traditions, which may provide the guiding light to the troubled world today. Abstracts are invited on the following sub-themes:

1) State and Governance in Dharma Traditions
2) Social Order in Dharma Traditions
3) State in Dhamma Traditions
4) Social Order in Dhamma Traditions
5) Ecology & Environmental Consciousness in Dharma Dhamma Traditions
6) Peace & Conflict in Dharma Dhamma Traditions
7) Dharma Dhamma Traditions in Gandhi, Ambedkar, Lohia and Deen Dayal Upadhyaya
8) Idea of Rashtra (Nation) in Dharma Dhamma Traditions

The abstract and the paper may be sent by email in word file (Unicode Format) to **dharmadhamma@indiafoundation.in**

Last Date for Submission of Abstracts: 30 September, 2017 | **Last Date for Submission of Papers: 05 November, 2017**