Centre for Advanced Strategic Studies

CASS JOURNAL

NATIONAL SECURITY NATIONAL DEVELOPMENT

VOL. 10 No. 2

ISSN 2347-9191

Centre for Advanced Strategic Studies
(CASS)

Journal

July - September 2022

Volume 10 No. 2

Edited by
Centre for Advanced Strategic Studies
M.M.D.W. Potdar Complex,
Savitribai Phule Pune University Campus,
Pune – 411 007
Telefax No.: 020-25697516
E-mail: cfass1992@gmail.com
Website: www.casspune.org

Published by
Centre for Advanced Strategic Studies
M.M.D.W. Potdar Complex,
Savitribai Phule Pune University Campus,
Pune – 411 007

For subscription, visit: www.cassjournal.in
Digital (Annual)..... INR 1900
Print (Annual)..... INR 3200 (incl. postage)
Single Copy ..... INR 900 (incl. postage)

For submissions and queries related to subscriptions and permissions,
write to : cfass1992@gmail.com

CASS Founder Members

- Late Shri PVR Rao, Former Defence Secretary, Government of India
- Late Shri RD Sathe, Former Foreign Secretary, Government of India
- Late Prof VG Bhide, Former Vice Chancellor, Savitribai Phule Pune University
- Late Air Marshal YV Malse, (Retd) Former Vice Chief of the Air Staff
- Late Shri Sharad Marathe, Former Industries Secretary, Government of India.
- Late Admiral JG Nadkarni, PVSM, AVSM, NM, VSM, (Retd) Former Chief of the Naval Staff
- Professor Gautam Sen, Former Head, Department of Defence & Strategic Studies, SPPU

Honorary Life Members

- Shri Abhay Firodia, Chairman, Force Motors Ltd
- Shri Atul C Kirloskar, Chairman and Managing Director, Kirloskar Oil Engines Ltd

Governing Council Members

- Shri MK Mangalmurti, IFS (Retd), Former High Commissioner, South Africa. Current Chairman, CASS, Pune
- Air Chief Marshal PV Naik, PVSM, AVSM, (Retd) Former Chief of the Air Staff, IAF
- Professor Gautam Sen, Former Director General and Member Board of Trustees, Indian Institute of Education
- Lt Gen Amitava Mukherjee, PVSM, AVSM, (Retd) Former Director General, Air Defence, Army Headquarters
- Lt Gen V G Patankar, PVSM, UYSM, VSM (Retd) Former General-Officer Commanding, 15 corps
- Air Marshal SS Soman (Retd), Former AOC-in-C, IAF
- Maj Gen Nitin P Gadkari (Retd), Former Commandant, College of Defence Management, Secunderabad
- Rear Admiral SS Godbole (Retd), Former DGNP
- Shri Shrinivasrao Sohoni, IAS (Retd), Former Advisor to Government of Afghanistan
- Air Marshal BN Gokhale, PVSM, AVSM, VM, (Retd) Former Vice Chief of the Air Staff, Air Headquarters, Presently Consultant, Principle Scientific Advisor, Government of India and DRDO and the current Director, CASS, Pune
- Maj Gen Shishir Mahajan SM, VSM, (Retd) Former General Officer Commanding 23 Inf Div and currently Deputy Director, CASS, Pune

INDEX

Air Marshal BN Gokhale (Retd)
PVSM, AVSM, VM
Director, CASS

Centre for Advanced Strategic Studies
Savitribai Phule Pune University Campus
Ganeshkhind Road, Pune 411 007, INDIA

Editor's Note

Prime Minister Narendra Modi recently commissioned India's first indigenously developed and built aircraft carrier INS Vikrant into the Indian Navy. It is the largest ship ever built in India. The Made in India ship is a significant boost to the Indian government's self-reliance initiative, particularly in strategic sectors. Ahead of the Air Force day, LCH Prachand was inducted in the IAF. The versatility and offensive potential of the copter is on a par or better than most attack helicopters operating globally. The LCH has stealth features. It can be used for offensive roles against enemy tank formations, infantry and also UAVs. The copter has built-in crashworthiness of landing gear, crew seats and fuel tanks. Addition of these two weapon platforms shows the progress made in the project "Atma Nirbhar Bharat"

Meanwhile the Ukraine Russia War has completed seven months and there is no sign of a Ceasefire. President Putin signed laws admitting the Donetsk People's Republic, the Luhansk People's Republic, Kherson region and Zaporizhzhia region into Russia in the biggest expansion of Russian territory in at least half a century. Even as the Kremlin moved to absorb parts of Ukraine in a sharp escalation of the conflict, the Russian military suffered new defeats that highlighted its deep problems on the battlefield and opened rifts at the top of the Russian government. The setbacks have badly dented the image of a powerful Russian military and added to the tensions surrounding an ill-planned mobilization. They have also fueled fighting among Kremlin insiders and left Russian President Vladimir Putin increasingly cornered. It will be interesting to see what happens next.

In this issue, Air Marshal Trikha discusses the trends in the Ukraine conflict in the second part of his article. Brig Mahajan in his piece on 2.5 front war recommends that instead of being prepared to fight a 2.5 front war, we should make our enemy fight on two fronts. Well researched articles on CBRN security in the Metropolitan region, Technology disruption and strategic contests and Emerging cyber security threats in India will update the readers on the latest technological issues. A tale of two buffers by Shri Jayant Umaranikar highlights that acceptance of Chinese claims over Tibet without settling Sino-Indian border, was a Himalayan blunder. India gave up her consulates and garrisons in Tibet, accepted Tibet as part of China, supported Chinese stand on Taiwan, lobbied for PRC to become Permanent Member of the UNSC and side-lined the Dalai Lama, without any quid pro quo. Infrastructure Development: An Engine for Defence Preparedness by Col Yogesh Nair tells us that good infrastructure adds teeth to the Armed Forces. Intelligence -First line of defence by Rear Admiral Nadkarni brings out that as with most cutting-edge technologies, intelligence collection and analysis systems can rarely be bought off the shelf, but have to be developed indigenously. Given that India has a large body of IT professionals and some of the smartest people in the world, there is no reason why we cannot do so. Finally the issue carries a book review of 'Fateful Triangle: How China Shaped US-India Relations during the Cold War'.

Wishing our readers a Happy Diwali and a Merry Christmas.

(BN Gokhale)
Air Marshal (Retd)
Director, CASS

CBRN SECURITY FOR A METROPOLITAN REGION

BY COL RAM ATHAVALE, Ph D

Introduction

Over the years, towns have grown larger into cities and metropolitan areas. They comprise residential areas, industries, corporate offices, large and small businesses and associated governance and administrative systems. The combination of these creates many toxic scenarios and polluted environments. Especially industries using a variety of chemicals, sewage treatment and waste disposal plants spew out toxicity in the urban environs. While much control and precautionary measures are invested in, we have seen major accidents in urban settings.

The horrors of Bhopal, India (1984) or Lac Mégantic, Quebec (2013), the countless boiler accidents, firecracker industry fires and the tons of toxic wastes that abound in our cities are enough to raise public paranoia. In addition to these horrors, port explosions and toxic fires like the Beirut Blast of 2020 and Tianjin Port explosions, China are a reminder of how toxic releases can devastate a city or part of it. A major CBRN accident or incident occurring in a city jurisdiction can wreak havoc and result in a multitude of casualties. Hundreds of helpless convulsing victims gasping for air surrounded by toxic gasses or vapours can seriously and rapidly overwhelm any response and healthcare mechanism. See the effects of COVID 19. The whole world got a terrible scare and even today many countries are battling the scourge of the pandemic. Wave after wave is having a devastating effect not just on the lives of people but on livelihood, business, and administrative capabilities.

Then there is the threat of a CBRN terrorist event. Deliberate sabotage of a research laboratory, or a toxic chemical plant or warehouse, causing a release in a crowded public place or high visibility event (a World Cup match or festivals like Eid, Christmas or Diwali) brings to mind horrors seen in Douma, Syria or Halabja, Iraq. The ongoing Ukraine war has raised the spectre of nuclear weapons being used on cities and towns, aka Hiroshima and Nagasaki. There

is even talk of Chemical, Biological and Radiological (CBR) threats and false flag attacks. It makes you ask the question, are our cities prepared for a mass toxic CBR incident? Or for that matter a Nuclear one?

While a nuclear war may seem presently unlikely, the threat exists like a sword of Damocles. The chemical and biological threats are very real as seen from the various incidents increasing with uncanny rapidity. There is no doubt that we need to be prepared to prevent, and if required protect our cities from such Chemical, Biological, Radiological and Nuclear (CBRN) threats. It needs deliberate and comprehensive actions by many stakeholders to effectively secure our cities. I have endeavoured to discuss the various steps and measures that should be taken for just such an eventuality.

Measures to Secure the Metropolitan Region

Contours of a Metropolitan Region.

The country can be divided into high density clusters of metropolitan regions. A metropolitan region is essentially an enlarged city with suburbs and outlying areas such as industrial parks, airports or ports, and even some smaller settlements absorbed by growing civilisation. It consists of large business districts, public transport hubs, critical infrastructures like seats of power, government buildings, historical monuments, tourist places of interest, sporting stadia and the vast residential complexes. Add to these the essential services that actually keep the region running namely water, electricity sewage, waste management and sanitary services. Then there are the logistics that help replenish and feed the households and businesses. This huge complex system has many risks and vulnerabilities. Before we look towards securing the region, we need to comprehensively analyse the risks and vulnerabilities. It will help us understand what are we securing the region against.

Risk Analysis and Vulnerability Assessment (RAVA).

The first step is to understand the types and magnitude of threats and risks. Each of the sub threats like chemical, biological or radiation need to be realistically analysed and assessed. Terrorist capabilities are ever-rising, and rapid and rampant industrialisation pose a myriad array of CBRN threats. These threats coupled with ill-planned urban infrastructural growth and overcrowding of cities lends to many risks and vulnerabilities.

RISK ASSESSMENT MATRIX	CONSIDER THE LIKELIHOOD OF A HAZARDOUS EVENT OCCURRING				
CONSIDER THE SEVERTY OF INJURYILLNESS	Very Unlikely to happen	Unlikely to happen	Possibly could happen	Likely to happen	Very Likely to happen
Catastrophic (e.g.fatal)	Moderate	Moderate	High	Critical	Critical
Major (e.g.Permanent Disability	Low	Moderate	Moderate	High	Critical
Moderate (e.g. Hospitalisation/ Short or Long Term Disability)	Low	Moderate	Moderate	Moderate	High
Minor (e.g.First Aid)	Very Low	Low	Moderate	Moderate	Moderate
Superficial (e.g. No. Treatment Required)	Very Low	Very Low	Low	Low	Moderate

Risk matrix based on Impact and Likelihood: Credits SiteSafe, Australia

Risk Zoning

Every city has an adjoining industrial area. Especially industries like pharma, plastics, paints, pesticides, and fertilizers. There would be many sewage plants and waste disposal areas. Some cities may have research labs handling toxic substances. There could even be a nuclear power plant in the vicinity. Ports and warehousing sectors (including container parks and large cargo transhipment facilities) may be storing tons of toxic chemicals or hazardous substances (remember Beirut, Lebanon or Tianjin, China). Risk Zoning is the technique of mapping risk areas, as given above, on a digitised map of the metropolitan region. GIS techniques (using vector and raster maps) are used to plot specific risk clusters on the map; they can be grouped based on localities, types, and levels of risks in clusters or zones. These zones should be numbered for easy reference. Additionally, risks should be graded based on type (chemical, biological, radiological, or explosive), impact (health, environment, business), severity, likelihood and kind of response. Such grading should take into consideration the Sendai Framework classification of manmade hazards.

(https://council.science/sendai-hazard-review).

Vulnerability Zoning

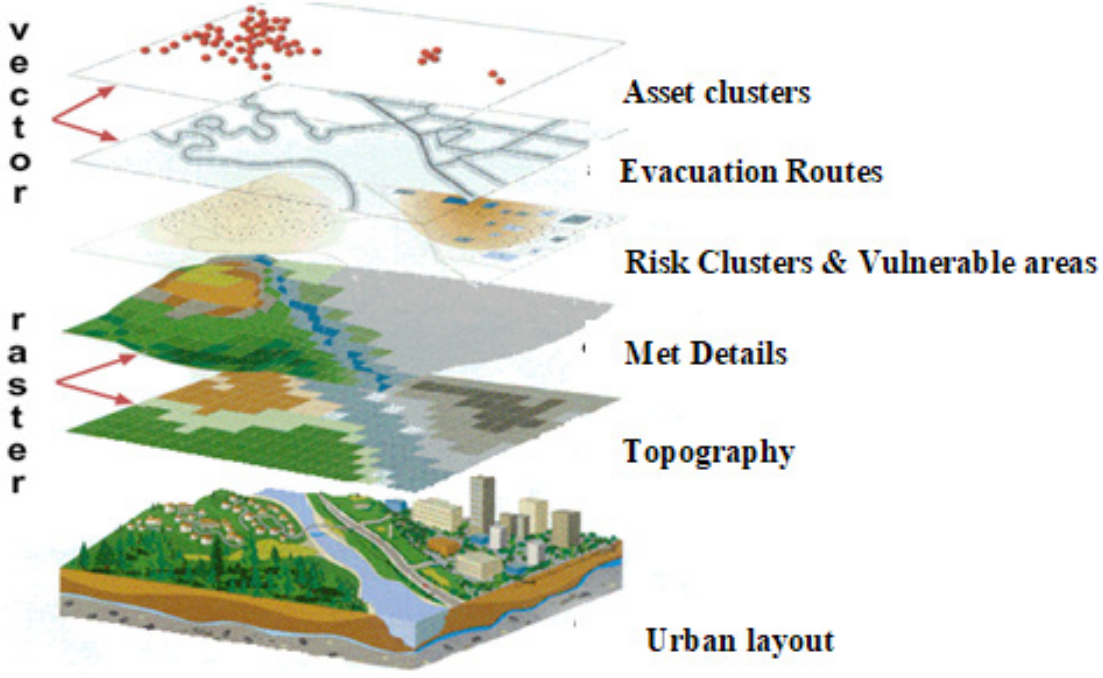
Critical infrastructures like water treatment plants, important government buildings, courts, airports, railway stations, metro stations, important public places, tourist spots and crowded/popular markets all are vulnerable areas in a city. These need to be included as a data layer in the vector mapping. Water bodies, their flow speed and direction should be mapped too. Toxicity in water bodies can lead to large areas of the city being vulnerable to contamination. Vulnerability will be dictated by the importance of the site, population density/ footfall and impact of a hazard manifesting there. These should be mapped as a digital overlay/layer to the risk zoning map.

Asset Assessment and Mapping

To protect and respond to any CBRN threat, there is a need for careful creation and assessment of assets. These could be infrastructural or in terms of human resource. The Government has established the National Disaster Management Authority. Under this agency there is a need for creating a nation-wide database (routinely updated) for managing the inventory of equipment, skilled human resources and critical supplies for emergency response. Primary focus is to enable the decision makers to find answers on availability of equipment and human resources required to combat any emergency situation. Such a database will also enable them to assess the level of preparedness for specific disasters. The database needs to be updated for CBRN related assets too. A realistic assessment of existing assets needs to be carried out. These should be also plotted as a layer to the risk and vulnerability vector plots. Different stakeholder assets like police, fire brigades, civil defence and available special response teams or paramilitary forces must be included. These should be clubbed in 'response clusters' on the plot. A study of the plots of risks and vulnerabilities as compared to the asset cluster plot will throw up anomalies in asset deployments (if any), in terms of rapid response capability to the risk and vulnerable zones. Further, the type of assets (human resource, transportation and equipment) and their imbalance in different asset clusters will also get highlighted.

Meteorological Assessment

The complete area under consideration should be analysed and mapped (raster mapping) for meteorological conditions. Wind speed and direction, ambient temperatures, ambient pressure, altitude, precipitation, and relative humidity assessments are important while analysing the likely spread of toxic contamination. Today we can have continuously updated met data with minute-to-minute specifics for ease of planning. Such parameters have effects on contamination spread and dispersion levels. Similarly, met conditions at varying times over a 24-hour cycle should also be mapped to analyse the temperature variations and inversion mechanics. This data can be sourced from the local met office, or the airport met department. Additionally, all critical infrastructure and high-risk facilities must have their own met sensors digitally networked to the hazard mapping system.



Representative image of GIS based mapping and zoning

Comprehensive CBRN Security Architecture

To enable and empower a metropolitan region to prevent and if required deal effectively with a CBRN incident the following needs to be instituted and executed.

- **Preventive measures**
- **Preparatory/precautionary actions**
- **Integrated Hazard Mapping and CBRN Control System**

Preventive Measures

After understanding and analysing risks and vulnerabilities, certain precautionary actions would go a long way in preventing and/or mitigating toxic risks from developing into disasters.

- **Distancing of Risk Areas.** Town planners must keep in mind the risk areas (like factories, warehousing, waste management and sewage disposal) and locate these well away from residential areas and other vulnerable areas as discussed above. In addition, while deciding the location of such high-risk facilities, meteorological inputs must be considered so that any possible release or exposure of toxicity flows away from the town and not into it. It should also be ensured that a clear perimeter of at least half a kilometre around such high-risk areas is kept free of residential complexes, slums, and labour colonies. Where existing high-risk areas have got surrounded by residential localities, the industry and the Government should consider shifting these to a safer location or creating a buffer zone and adding enhanced safety measures to avoid any hazard.
- **Legislative Mechanisms -** Laws and Acts for CBRN. CBRN incidents can cover a wide spectrum from natural to manmade (industrial, logistics, medical) to terrorist incidents. The State needs to develop and refine existing laws and acts to ensure due prevention of CBRN incidents. Further, laws to cover all stages of toxic substances from creation/import to disposal need to be framed and executed. Laws must give out the prosecution aspect to ensure compliance. Some laws need regulations and SOPs to be developed by next rung of administration. All such laws, acts and regulations need to be backed by implementing, executionary and oversight mechanisms.

- **Strict Oversight and Audit.** All high-risk facilities are required to follow a strict safety protocol. Such oversight mechanisms are mandatory in all facilities. While the in-house Health, Safety and Environment (HSE) managers and their team would be responsible for ensuring the safety of workers, staff and equipment, the Government has instituted laws and regulations for occupational safety and mandated third part safety and security audits. These if done diligently and as per the required schedule can minimise the risks and help maintain good safety standards. Global industrial or workplace (industries, trade and commerce, logistics and waste management) safety best practices like regular third-party audits, oversight mechanisms and, Globally Harmonised Labelling System (GHS) need to be assiduously adopted.
- **Surveillance and Early Warning (EW).** As part of the safety protocol at all high-risk facilities and at important vulnerable areas, suitable early-warning sensors need to be deployed. The sensors, fixed or mobile (vehicle, drone or robot based) would carry out 24/7 surveillance over the risk areas. Such sensors would detect toxic release or spread in real-time mode and trigger alarms. These alarms would be networked for necessary actions (simultaneously by multiple stakeholders) as explained in subsequent paragraphs. In addition to the alarms at high-risk facilities and critical infrastructures, the Metropolitan authorities need to institute a set of standard automated alarms or warnings over multiple media to pre-warn the citizen about an emerging threat.

Preparatory/precautionary actions

Post a detailed RAVA and instituting necessary preventive measures, there is a need to plan and prepare for a possible CBRN threat. The main aim of such actions is to limit casualties, prevent escalation of the threat and minimise its effects. Some key preparatory and precautionary activities are discussed below.

- **Asset creation.** There is a need to create the right assets to be able to protect people and respond effectively to the emerging threat. The assets can be infrastructural, research and suitably equipped human resource.

    - **Infrastructural Assets.** There is a need to create and improve certain key infrastructural assets. In most parts of western Europe, the metro train stations and tubes are well underground, enabling them to be used

as temporary sheltering means in a CBRN attack. Similar sheltering measures need to be instituted in cities, under critical infrastructures and industrial parks. Other than such large underground shelters, strong overground facilities and buildings that can be used as temporary sheltering need to be studied and upgraded with sealing and clean air systems. In addition to these, residential societies and public facilities (malls, administrative and corporate infrastructures) which have secure underground parking can well be converted to provide such secure sheltering. All critical infrastructures need to create temporary stay-safe chambers or rooms with independent Heating, Ventilation and Air Conditioning (HVAC) systems (including CBRN filtration). Secure in-house power sources for any widespread power disruptions (could be due to power grid failures or EMP strikes by adversaries) need to be installed. Suitable evacuation routes and assets will need to be planned for shifting people to safer places once the situation permits. The Ukraine crisis has brought out many lessons in temporary sheltering of the citizens in heavy attack scenarios. For CBRN protection, sheltering facilities will need sensors, alarm systems, sealing mechanisms and CBRN filtration systems for clean and secure environments.

- **Sensors and Detectors.** There is a need to deploy static and mobile sensors and detectors for surveillance of critical infrastructures and high-risk areas for possible threats. These will help prevent a CBRN incident. All high-risk facilities must have such systems. There are many fixed and mobile detection and early warning systems available in the international market. Most of these are used in a networked manner with automated hazard prediction and early warning systems. More about this below.
- **Research and Forensics.** State of the art research and forensic capabilities are a must for effective prevention and response to a CBRN incident. High containment and secure laboratories to analyse and develop antidotes, drugs and vaccines are needed. While some laboratories do exist, there is a need to increase footprint and enable all major cities with such analytical facilities. Similarly, forensic laboratories to rapidly identify and analyse contamination in an interventional or response situation can be a huge asset in escalation prevention and minimising casualties. For an effective response, there is a need to also create, at the Metropolitan level, mobile laboratory assets (field laboratories) for rapid deployment at the incident site. Such CBRN mobile laboratories are being developed by some vendors.

- **Human Resource.** The key component in any preventive intervention or response to an emerging CBRN incident is the human resource. Response teams of suitably trained and equipped personnel are essential. Many stakeholders would be part of any intervention or response scenario. The Armed Forces do maintain well trained and equipped CBRN Quick Reaction Teams for battlefield requirements, however there is a need to build on-site response teams at all high-risk facilities to avoid response time lags and increase response footprint. These could be part of the on-site security and staff manning such facilities. In addition, the security staff at all critical infrastructures and important public places, local police, fire brigades and Civil Defence personnel, all need to be adequately trained and equipped for immediate mitigation and escalation prevention. Basic awareness and mitigation training should also be imparted to private security staff in residential areas with local volunteers (preferably from within the Resident Welfare Associations [RWA], residential societies or resident committees) supplementing such assets. The importance of Civil Defence and local volunteers in saving lives has been demonstrated in the Ukraine crisis and in many instances in India too.
- **Training and Equipping.** Without optimal training and adequate equipment, no response can be successful. Especially in CBRN scenarios, standardised basic training needs to be instituted. Training is required for all stakeholders. CBRN training can be graded from basic to advanced as also based on the need for different levels of application from administrators and decision makers to first responders. Hence, there needs to be a central institute or centre that imparts the training. CBRN equipment is expensive, especially sensors and detectors. Therefore, correct operation, fitment and due maintenance must be inculcated in the personnel who are to use these. Training aids like simulators and virtual reality or augmented reality (VR/AR) systems should be used. There are companies that make such training aids for safety and enabling the users. The VR/AR aids can be customised for specific requirements like use of detection equipment, wearing of protective gear, decontamination techniques and also for medical management in field.
- **Critical Equipment Production and Emergency Stocks.** COVID 19 hit us all in early 2020. Simple things like masks and sanitizers were considered fashion accessories of rich people. As COVID 19 struck,

suddenly there was a scramble for these items. Of course, there was a dearth of PPE, ventilators and even hospital beds. Critical medicines stocks were low and there was general panic. Fly by night businesses began cashing in on locally made PPE, masks and sanitizers. Some entrepreneurs also resorted to flash imports. Quality was grossly ignored till the concerned authorities published norms and standards. In a mass CBRN situation, there will be a short-term yet sudden need for such critical items in great numbers. There is a current system for emergency stocks for natural disasters. This system should be enhanced with CBRN related stocks in these stores. Planned CBRN equipment stocks at select strategic locations within easy access to various cities and the capability to ramp up production in a crisis are needed. Holding stocks is a costly affair. Due care should be taken to review stocks based on market availability and the residual life of these lifesaving items.

- **Essential Drugs and Antidote Stocks.** As in the case of critical equipment, essential drugs and antidotes need to be stocked for critical CBRN situations. The need for such stocks shall be immediate and due consideration and planning must be undertaken for their rapid deployment in the affected areas. A periodic review with pharmaceutical companies must be undertaken to ensure optimal availability and production dynamics in case of emergent large-scale requirements. Public-private research partnerships to revise vaccine and antidote policies and aid in the development of newer and better vaccines based on anticipated demand for emerging threats must be catered for.
- **Sensitizing Stakeholders and Populace on CBRN Threats and Their Mitigation.** The most important preparatory or precautionary action is to create and enhance awareness about CBRN threats and mitigation measures. Today, despite COVID 19 raging in the environment for two years, the level of awareness and understanding is low. We need to organise awareness workshops for all possible stakeholders. Government agencies like home, police, hospitals and healthcare, municipal services (water, fire, emergency services, sewage, waste management, crematoria), paramilitary forces all need to be adequately sensitised and trained. Sensitizing citizen including students and workers is essential. Sensitisation using well-structured campaigns on social media, print/digital media and/or FM radio jingles can be considered. We also need to train School & College students

in understanding the basics of CBRN risk mitigation. Due emphasis is needed for training and sensitizing the staff and workers of industries and logistics agencies (transportation, warehousing and bulk handling). Again, the need for a central CBRN Institute to standardise, coordinate and structure such workshops and training is felt.

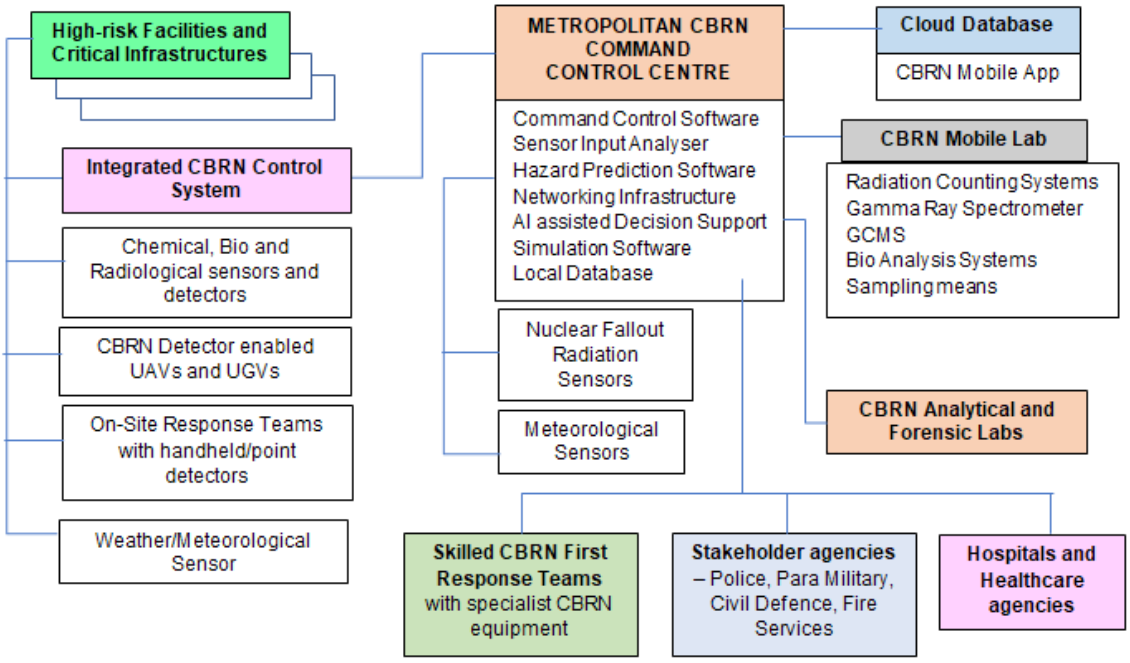
Integrated Hazard Mapping and CBRN Control System.

Keeping in mind the requirement of managing the multifarious CBRN detection and sensor deployments at high-risk facilities and critical infrastructures, there is a need to integrate these into a single command and control system at each metropolitan regional headquarters. The Government has already put in place a security based networked system. We need to expand such initiatives to include an Integrated CBRN Control system.

- **The System Architecture.** The Integrated CBRN Control system is a digitised platform wherein all CBRN sensors and detectors (early warning) are networked to a control station. Each high-risk facility and critical infrastructure should have such a control station. This should should be integrated with the Integrated Metropolitan Command and Control Centre. The System has the following parts:
  - Sensor data receiver and analyser
  - Meteorological
  - Hazard Prediction with automated warning system
  - Decision support system
  - Resource inventory control

- Every high-risk or critical infrastructure should have a set of deployed sensors (both fixed and mobile depending on the layout and sensitivity of the venue). These should be networked into a local Command and Control station that can process the incoming data from the sensors. The high-risk facility or critical infrastructure control station receives real-time inputs of any releases, spills, or contamination spreads in their areas. The inputs (including meteorological) are plotted on digitised maps and a hazard prediction map is generated. The system also makes identification and intensity assessments based on the inputs and assisted by Artificial Intelligence (AI). Based on the areas affected or likely to be affected,

automated warnings are relayed to the nearest response asset as per the mapping discussed above. Hazard mapping, situational reports and warnings are also relayed to the Integrated Metropolitan Command and Control Centre for alerting neighbouring localities and response assets. Associated stakeholders like the fire department, hospitals, police, forensics and others also get these warnings. Artificial Intelligence (AI) enabled Decision Support module of the Integrated Metropolitan CBRN Command and Control Centre gives suggested protection and mitigation measures to response teams and assists in directing forensics for early analysis. It also gives predicted figures needing hospital care and helps in the immediate planning of equipment and antidote/drug requirements. Alerts are sent out to hospitals in the vicinity and to the metropolitan health department.



Representative System Diagram of the Integrated CBRN Command and Control architecture

- **Sensor deployment.** There is a need to deploy a select range of CBRN detectors and sensors. These need to be identified based on location, type of threat envisaged, usage (fixed, roving or handheld) and optimal coverage. Stand-alone detectors can be deployed at key locations within and on the periphery of the facilities. A coverage modelling based on spread dynamics of likely threat releases can be developed for each location to optimally deploy such detectors. In addition, autonomous or partially controlled roving sensors and detectors can be planned for larger venues covering open grounds and clustered risk facilities. Such autonomous roving systems can be unmanned aerial vehicles (UAVs or drones) or unmanned ground vehicles (UGVs or robotic systems) with an onboard array of CBRN detection devices. Highly critical infrastructures may even have roof or mast mounted Stand-Off detectors capable of detecting approaching chemical threats from up to five kilometres. For pinpoint identification of the release/hotspots, handheld systems can be used by the response teams or Unmanned Ground Vehicles (UGVs) can be deployed for random coverage surveillance and for hotspot verification.
- **Alarm Mechanism.** The Integrated CBRN Control System will have an alarm mechanism included. The alarms would be audio-visual indicators with coding to indicate the type of hazard. The alarms can be transmitted not just to the facility-based control centre but also the main centre at the Metropolitan control room.
- **Alert and warning messages.** The Integrated CBRN Control Centre can generate automated user-specific alerts and warning messages. These would be updated as the situation unfolds and transmitted automatically to the concerned recipients.
  - **Stakeholders.** Various stakeholders who would need to be alerted would receive regular situational updates and alerts. These messages would be specific and contain hazard details, contamination spread predictions, actions at hand, mitigation measures and suggested further actions. Stakeholders can use these inputs to initiate precautionary and protective actions for as yet unaffected areas.
  - **Public.** Cautionary messages can also be generated by the Integrated CBRN Control System for the common public. These can be suitably integrated to be transmitted via social media, television and radio broadcasts. AI-generated Do's and Don'ts for mitigating the effects of the hazard can also be included for the specific type of hazard in these cautionary messages.

Representative image of an Integrated CBRNe Command and Control Centre. With permission of M/s Nucleonix Systems, Hyderabad, India.

- **Enhancing protection.** Certain aspects of mass protective measures have been discussed under asset creation above. In addition, some measures that could be undertaken to enhance protection levels are discussed below.
  - **Escalation Prevention and Containment.** Rapid escalation prevention and containment of the toxic release is of utmost importance. All high-risk facilities and critical infrastructures management must cater for mechanisms and drills for the same. Necessary immediate assistance equipment and stores should be stocked at all high-risk facilities and critical infrastructures. Staff and workers must be trained for all possible contingencies and prepare for the same.
  - **Collective Protection.** Every high-risk facility and critical infrastructure must cater for onsite protection for the staff and workers. Key installations may plan underground bunkers/holding rooms for the security of VIP and critical assets. For general public, underground assets like parking spaces, metro stations and tunnels or basement areas in Malls, hospitals and any other public infrastructure can be suitably modified for use. Due attention to the sheltering capacity, duration of stay and connected logistics must be given. Protected evacuation means and alternate routes need to be planned for various contingencies. First-aid measures should be catered for. Members of the staff who have a proclivity for nursing or first aid should be suitably trained. Similar selection and training are needed at residential societies. Volunteer members from resident committees can be trained. Where localities exist with no resident committees, local district offices must be tasked to do the needful. Signposting of essential helplines and nearest shelter

details. Plans should be developed at Metropolitan levels to convert a few metro/subway coaches or air-conditioned busses suitable augmented with CBRN sealing and filtration means.

- **Individual Protection.** As mentioned earlier, all stakeholder teams who may form part of response or intervention in CBRN incidents need to be suitably kitted out for optimal protection. CBRN suits, masks and Self-Contained Breathing Apparatus (SCBA) sets need to be provided. New technologies to lessen the physiological burden on the wearer and giving enhanced protection must be incorporated. There is a need to also stock a minimum number of kits (PPE and respirators) at all high-risk facilities and critical infrastructures, based on anticipated usage. The administration should widely distribute a booklet/handbook on CBRN Emergencies, which should include dos and don'ts for the common public. Simple protective and mitigative actions must be included in such booklets/handbooks. For wider distribution, schools and colleges and public places like malls and cinema halls can be used. Basic contents can be displayed at public places, malls and residential complexes.
- **Decontamination.** It is very essential to decontaminate even suspected items, body parts and equipment to avoid secondary contamination and save lives. In any CBRN incident which entails mass contamination, the Administration would set up centres for decontamination. Large vehicle wash centres can be quickly converted to effective decontamination stations.
- **Mass Decontamination.** A CBRN incident would affect a large number of people. In such instances, mass decontamination of the affected or even suspected of contamination would be required. There are procedures and drills to set up such mass decontamination centres at selected locations. These would need a huge supply of water and an open area which can accommodate the number of people to be decontaminated. Normally a shower washdown with clean water and a decontamination solution is the norm. It needs to be understood that all belongings on the person like watches, phones, jewellery, documents and clothing may need to be discarded and either incinerated or separately decontaminated. Therefore, a fresh set of clothing including footwear may need to be provided to those undergoing decontamination. Decontamination logistics are intensive and need to be planned with care. It is also recommended that all high-risk facilities and critical infrastructures maintain an on-site decontamination centre

suitably located after threat appreciation. Necessary logistics for such a decontamination centre should be the responsibility of the high-risk facility and critical infrastructure. Open areas, public parks and vacant plots can be earmarked for decontamination areas.

- **Individual Decontamination Kits.** As with the protective kits, a similar number of personal decontamination kits should be catered for at all high-risk facilities and critical infrastructures. These are small easy to use decontamination pads with powder substances. Such personal decontamination kits are also needed by all stakeholder response and intervention teams. Sanitiser sprays and gels can also be included for decontamination of personnel and equipment.

- **Medical Management.** CBRN incidents can lead to hundreds of casualties. Many victims may need critical care and careful yet immediate management. Key issues required to be addressed would include:
  - **Triage.** This is the procedure to identify the victims requiring prioritised care. Doctors and paramedics are trained to conduct triage in mass casualty situations in the field. All hospitals and clinics need to prepare for CBRN incidents and cater for adequate Triage equipment. Suitable training if required may be imparted under the Continuing Medical Education (CME) programs.
  - **Evacuations.** Detailed planning is required for the evacuation of victims from the incident sites. An adequate pool of available ambulances needs to be maintained as a database with the Metropolitan Administration. A dedicated communication plan to requisition ambulances with paramedic staff must be worked out. A well thought out private-public coordination for such ambulance and staff provisioning must be instituted. Such drills must be practised. Metropolitan planners must also work out routes of evacuation (including alternate ones) from all high-risk facilities and critical infrastructures.
  - **Hospital Preparedness.** Careful planning and preparation are needed to enable hospitals and clinics to manage CBRN casualties. Hospitals would be called upon to deploy field medical aid centres near the incident site(s). Tents, field operation and treatment facilities, equipment like resuscitators and CBRN casualty pods are required to be catered for. Doctors and paramedics must practice rapid deployment of such field facilities and hospitals must train the support staff for the same. Every city has a medical helpline. Such facilities should have the capacity to switch to a CBRN mode on the requirement. Necessary additional

supplies and modification kits should be provisioned.

- **Mass Crematoria.** As the fatal casualties would be toxic and contaminated, there may be a need for the contained disposal of these cases. As such, special crematoria may be earmarked for such procedures. In some countries, mobile container-based crematoria are provisioned for onsite disposal.

- **Control Agency and Incident Command.** CBRN situations need multi-agency response and interventions. You cannot have all stakeholders operating in their own way without coordination. There is also the need for centralised command for effective operations. It is necessary to have a central control agency under the Metropolitan administration. This agency should coordinate all preventive and preparatory actions including planning and follow-on tasks. Further, for onsite operational effectiveness, an Incident Command Centre is needed to be set up. Guidelines for an Incident Command have been issued by the NDMA.
- **Guidelines and SOPs.** For the smooth and seamless functioning of all the stakeholders in a CBRN situation, there is a need for setting guidelines and Standard Operating Procedures (SOPs). The Metropolitan agency made responsible for CBRN incident management should be tasked with developing and disseminating such guidelines and SOPs amongst all stakeholder agencies. Many States and Districts have developed SOPs based on guidelines issued by central agencies and ministries.
- **TTE and Mock drills.** For effective operationalisation of intervention and response plans, there is a need for practice. Especially as there are many stakeholder agencies involved. Based on the guidelines and SOPs, regular Tabletop Exercises (TTE) must be conducted based on different CBRN contingencies which are possible. Once the plans are discussed and played through in TTEs, finalised contingency plans need to be developed. Such plans need validation on the ground. For this, mock drills are a must. It should be ensured that all relevant stakeholders participate in such mock drills. Due diligence and realism, within safety and security limits, should be built in to suitably train the personnel.
- **Review mechanism.** No plans and situations are permanent. Threats are constantly evolving. So is the technology and newer equipment. It is, therefore, necessary to review the plans and training procedures periodically. Guidelines and SOPs may need revision. Such reviews are essential to maintain optimal capabilities to prevent and if required effectively respond to a CBRN incident.

Conclusion

Smart cities need to be smart secure too. Many cities in Western Europe have systems in place for CBRN risk mitigation. It may be said, and is true, that most regulations for the above system exist even in India. However, implementation has been a bane. Residential areas have enveloped industrial zones and vice versa. Industrialisation and uncontrolled urban development have created an ever-growing range of CBRN threats. Metropolitan authorities, the various stakeholder agencies and the public at large need to be sensitised and prepared to prevent such threats. At the same time, due precautionary measures and mitigating procedures need to be comprehensively instituted to save lives and prevent escalation of CBRN incidents. It calls for a structured program cooperative initiative duly guided by experts in the field. This paper is a suggested way forward and an appeal to Metropolitan, District and State authorities to take note and enable our cities. Let us make our cities CBRN secure.

ABOUT THE AUTHOR

COL ATHAVALE

Col Athavale has been a Key Adviser to the Government of India (MoD and MHA) on CBRN Security. He has been a Key CBRN Expert for the EU CBRN Risk Mitigation Centres of Excellence initiative in Eastern and Central Africa. A Visiting Faculty at select Indian and overseas universities, prolific writer and a speaker in international seminars and conferences on CBRN subjects, he holds a PhD in CBRN Security and Incident Management. He has authored a pioneering book titled “Toxic Portents” on ‘CBRN Incident Management in India’. Presently he is a freelance CBRN Security and Risk Mitigation Consultant based at Pune, India. His personal website https://chebiran.com has more details

TECHNOLOGY DISRUPTION AND STRATEGIC CONTESTS

BY AJEY LELE AND KRITIKA ROY

AjeyLele is a Consultant at MP-IDSA, New Delhi, India and Kritika Roy is a Researcher at DCSO GmbH, Hertie School, Berlin, Germany

In the current era of Industry 4.0, it has been projected that Disruptive technologies are likely to impact the normal operations of a market/industry. Particularly, the defence industry is expected to witness a major revolution. 'Data' often gets regarded as 'new oil' for the modern day world which is found increasingly becoming data-driven as Information and Communication Technologies(ICT) are getting intertwined with all critical systems and infrastructures of a nation. There is an evident impact of the convergence of several technology trends along with the exponentially increasing volume of data that doubles every three years as information pours in from various sources. Simultaneously, the data storage capacity has increased, while its cost has plummeted. Data scientists now have unprecedented computing power and technology at their disposal, and they are devising ever more sophisticated algorithms. While "data itself will become increasingly commoditized, value is likely to accrue to the owners of scarce data, to players that aggregate data in unique ways," and especially to providers of valuable analytics.[1] Data has become a strategic commodity which is often referred to as oil on which future wars might be fought. This very data could be used as well as misused. This has generated a new kind of fear in the minds of men – the ability to use data to wage dedicated information warfare.

Moreover, the need to leverage the potential of rapidly expanding data, led to the evolution of unique techniques and technologies for data storage, analysis, and visualization. Especially with many countries moving towards the concept of centralized databases (where the digital identity of an individual is stored at a single place), these databases could become easy targets of misuse. Advances in technology such as Additive Manufacturing (AM or 3D

Printing), Big Data Analytics, Cloud Computing, Smart Factories, Block chain, IoT (Internet of Things) and quantum technologies brings forth unforeseen opportunities as well as challenges.

This paper targets to comprehend that if such technologies are likely to disrupt the existing technological base of the defence industry and bring in change to the technology trajectory owing to the possibility of the likely arrival of the data-driven world. Additionally, the paper critically analyses the potential of new technologies of Big Data and IoT that involves latching together isolated data flows coming from potentially every nook and corner of the world. This progress could have critical implications, specifically between those whose data are included and those whose are excluded, and between those who have access to the data and those who do not.

The Ever Changing Technology Trajectory

The world has undergone three fundamental technological revolutions. Beginning with the invention of the steam and hydraulic machines then moving towards an age of mass production. The third revolution saw the emergence of electronics and information technology (IT) that found application in varied industries. Today, we are standing at the cusp of the fourth Industrial Revolution or Industry 4.0that is, characterised by the widespread application of cyber-physical systems. A new era in intelligent network systems, big data analytics, IoT, cloud computing and biotechnologies is demanding more amount of use of data. The fundamental aspect of Industry 4.0 has been the development of digital, physical and biological technologies.[2] Not only major breakthroughs have been achieved in these arenas but also fundamental progress have been made with the crossover within and between these technologies.

Several trends in the development of technology have led to the current technology trajectory and the most important has been the growth in digital technology. This, in turn, could be attributed to the exponential growth of the computing power that continues to be in line with Moore's Law which states that" the overall processing power would double every year." [3] Moreover, the increasing integration of hardware over networks magnifies the capabilities of the individual pieces of hardware that the network connects.[4] Furthermore, the advances in software have allowed sophisticated mechanisms for the extraction of information from the data that are stored, either locally or on the network.

Interoperability has been another important driver for digital growth along with standardisation of components and systems facilitates the connection of different companies and sectors.[5] Advances in optical fibre cables (OFC) has also facilitated and improved connectivity which in turn has allowed the smooth connection of different smart devices. From the network point of view, broader bandwidths combined with new algorithms for traffic surveillance has improved transmission capability. The influx of new users and more capacity demanding services have paved the way for massive investment in buildup of several networks, service development a continuous upgradation of systems.

Another major factor has been the emergence of Internet 2.0. This has a direct impact on efficiency and productivity in all sectors and on all levels. Internet is a pipe for delivery of content and ideas.A free flow of information can bridge the gap between cultures and organization and enhance the level of flexibility. Overall improved communication and connectivity also facilitate the creation of global production networks and global innovation networks.

It is also important to note that particularly for the technologies like the IoT essentially require small datasets. A Small data is a dataset that contains very specific attributes which are used to determine current states and conditions or may be generated by analyzing larger data sets. Normally, small datasets provide real-time information. Normally, it has been noticed that current state of a handful of attributes are sufficient to trigger a desired event. [6] Actually, every time it is not the quantity of the data which is of great importance, but is of importance is the quality of data. Having a bad data in abundance is of no use. Hence, there is also a view that the data should be Smart Data.

Technology Innovation and Disruption

The twenty-first century is seen as an era of uncertainty and complexity because of the rapid changes the world is undergoing. Factors like globalization and technological changes are expediting the process in areas of business, education and society. Innovation is a refined version of an original invention leading to enhanced growth and profit of an organization.[7] Owing to the transformational impact on industries, innovation has become the new imperative in all arenas.[8] It forms the basis of demarcation between leaders and followers as the competition for finding a more workable solution for complex problems keeps increasing.[9]

Disruption, on the other hand, is defined as the displacement of existing technology or market. It is an act that leads to systemic changes, while

innovation usually has more positive connotations and is correlated with upgradation. Innovation is seen as a rational process while disruption is considered unpredictable, irrational and damaging. This does not necessarily mean it is always a negative thing, in fact, some people consider disruption a higher form of innovation.[10] Various industrial agencies are constantly keeping a track on the happenings within technology and business domains. This allows them to judge early trends and recognize the possibility of disruption. Finally, all this helps them to plan and adopt an active business strategy catering for possible disruption.[11] The next generation of innovative technologies promises to be even more disruptive. For instance, machine learning and deep learning capabilities have an enormous variety of applications that stretch deep into sectors of the economy that have largely stayed on the sidelines thus far.Data and analytics have altered the dynamics in many industries, and change will only accelerate as machine learning and deep learning develop capabilities to think, problem-solve, and understand language. As we enter a world of interconnected systems, self-driving cars, personalized medicine, and intelligent robots, there will be enormous new opportunities as well as significant risks—not only for the entire industrial setup but for society as a whole.

Understanding the Power of Data

The types, quantity and value of data being collected are vast: from personal profiles on sites like Facebook or LinkedIn to demographic data, from bank accounts to medical records to employment profiles. Firms collect and use this data in order to monetise it by tailoring their services. Governments, in turn, use data to provide critical public services more efficiently and effectively. Researchers use it to speed up the way they develop new solutions, drugs and treatments. Often the disjointed siloes of data are mapped together and coupled with the recent advancements in Big Data and IoT for profiling and deeper insights. Thus, data has become a potent driver for change, growth and success.The sheer volume of data generated by individuals and organisations across the nations have made the adoption of a data-led culture an important priority. Countries are investing in transformation initiatives to establish a “data culture” within their organizations.[12] There is a prevalent realization that a data-driven approach is imperative to enable better public engagement and experience, reduce operational expense, mitigate risk, increase organizational efficiencies, and identify new opportunities, markets, products and services.

The opportunities that data brings are phenomenal. Deeper insights into data is used to understand popular trends that help in making a better decision. It encourages a result-driven environment as one could easily decipher what works under what conditions while ensuring improvement through viable feedback loops. Data-driven decision-making has multiple advantages, such as better understanding of the situation at hand (due to the availability of past data and prediction data), assessment of alternative solutions, and mapping it against the best possible outcome, which makes processes more agile and facilitates better-informed decisions.[13]

However, the emergence of a data driven world has also facilitated the fear of "Data Colonialism." Colonising a country no longer requires its physical invasion with military strength but can simply be done by activities like controlling through networks and databases with a click of the cursor. Just as historical colonialism paved the way for industrial capitalism, data colonialism is paving the way for a new stage of capitalism whose outlines is only partly seen. In this data driven era, there will be no part of human life, no layer of experiencethat cannot be extractable for economic value. Human life will be there for mining by corporations without reserve as governments look on appreciatively.[14] This process of capitalization will be the foundation for a highly unequal new social arrangement, a social order that is deeply incompatible with human freedom and autonomy.[15] Data colonialism justifies what it does as an advance in scientific knowledge, personalized marketing, or rational management, just as historic colonialism claimed a civilizing mission. Data colonialism would be global, dominated by powerful states, like the USA and China. The result is a world where, wherever we are connected, we are colonized by data. This online data dominance is fortifying the "hegemony of multinational corporations" over individuals all around the world. Over a period of time, territorial borders may not decide control over people or their nationality rather, control over data will.[16] The future of humanity would be decided by who owns how much of our data.

As digital communications become ubiquitous, data will rule in a world where nearly everyone and everything is connected in real-time.[17] Stakeholders will need to embrace uncertainty, ambiguity and risk. There is a visible trade-off where some aspects of personal privacy would be sacrificed in order to benefit. Tensions regarding the misuse of digital data would be on a rise. Fundamental questions about privacy, property, global governance, human rights – essentially around who should benefit from the products and services built upon digital data – are major uncertainties shaping the opportunities. Too often governments and industry see new opportunities: for surveillance,

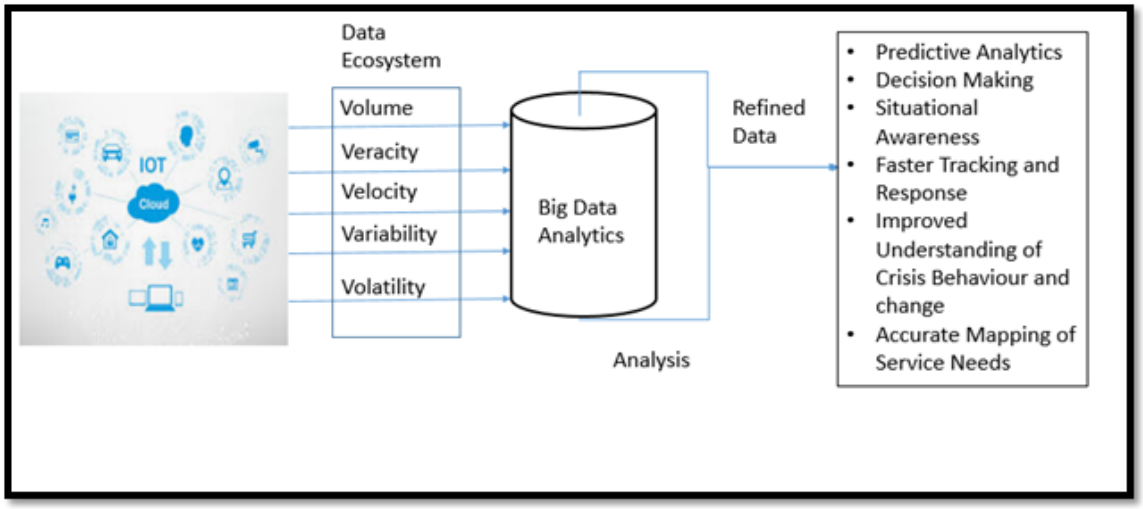
income generation, and control. There are few safeguards in place. The drive for these changes is strongest in emerging economies where legal and technical safeguards are weakest and there is little to no transparency of decision-making processes, and limited rule of law and the responsibilities of the private sector are blurred.[18] The innovations in policy and technology are largely left unregulated and unchecked. This will have significant ramifications for privacy and will transform the exercise of power, creating new possibilities for oppression, strengthening existing inequality, discrimination, and exclusion, and potentially leading to new forms.

Assessing the Impact of Different Technologies on Data

The phenomena of collecting and collating a large amount of information are age-old; however, the practice called 'big data' is relatively new. The "Big" here refers to the bulkiness of various aspects of the structured or unstructured data that includes volume, veracity, velocity, variety and volatility.[19] The bigness of big data is also associated to the "newly expansive capabilities to connect disparate datasets through algorithmic analysis, forging unpredictable relationships between data collected at different times and places and for different purposes."[20] Part of the data distribution and collection is facilitated by the manner in which all types of machines and devices interact, communicate and learn from each other.We are slowly moving towards a connected life with connected cars, smart homes, wearables, smart cities and connected healthcare.[21] This is facilitated by IoT which consists of two foundational things, first, the internet itself that encapsulates a gamut of information and communication technologies. Second, includes a collection of semi-autonomous devices that leverage inexpensive computation, networking, sensing and actuation capabilities in uniquely identified implementations to sense the physical world and act on it.[22]

IoT is a collection point for data, while Big data analytics is a key to analyze IoT generated data from connected devices which helps to take the initiative to improve decision making (as shown in the figure). Besides Big Data and IoT, the crossover of various technologies like cloud computing, artificial intelligence, blockchain makes various processes cost and time effective by facilitating quicker decision making, pattern detection and predictive analytics for humans.

Figure: Use of IoT and Big Data in Data Analytics



With the increasing pace of technology development, there is a possibility that in coming two to three decades the world would consist of interconnected machines that will not only make human life easier but also make it cost, time and energy efficient. Technologies like AI (Artificial Intelligence), Big Data, Cloud Computing, IoT, Blockchain, 3D Printing are likely to shape the world that has been never envisaged before. The following section provides a broad overview on some of these technologies which are also expected to impact and alter the battle landscape of tomorrow.

Few Disruptive Technologies at a Glance

The major idea behind Industry 4.0 is to bring together information, resources and people and integrate new concepts into industrial processes to improve value creation, work organization and downstream services. In essence, facilitating the generation of customer-specific designs, bringing in flexibility through networking, establishing improved decision-making and ensuring adaptation of resource consumption and establishing a system for interactive collaboration of workers.[23] Technologies that are paving the way for the establishment of Industry 4.0 have made significant advances and are finding applications in both civil and defence sphere. There are various technologies which presently are at the different levels of development. Some the most debated technologies are discussed below.

AIrefers to the ability to make machines act intelligently.AI has emerged more as an umbrella term encompassing intelligent robotics, ambient intelligence, machine automation, autonomous agents, reactive and hybrid behaviour-based systems and big and small data. The unique feature of AI is that it is self-adaptive and uses progressive algorithms, which allows self-programming by recognizing structure and regularities. Since data is at the heart of AI programming, the more accurate the data, the more accurate is the system.[24] The virtue of autonomy itself can be facilitated by AI, by means of studying patterns and regularities and then coming down to specific decision making. In the military milieu, the development in the field of AI would facilitate both enhanced and cost-effective capabilities in different spheres.

Cloud computing is a means of retrieving information and services from the Internet through web-based tools and applications, as opposed to a direct connection to a server. The data stored to the cloud, are easily accessible but only through a continuous access to the internet. In the last few years, several countries have been integrating cloud computing to the C4I (Command, Control, Communications, Computers, Intelligence) systems in order to provide more cost-efficient and effective services to units in remote locations as well as operational and tactical units under deployed conditions.[25] In future war fighting, cloud computing is expected to facilitate reliable access to information, simplicity to deploying units, increased possibilities for virtual training.

Blockchain is basically a public electronic ledger that facilitates the creation of an unchangeable record of their transactions, each one time-stamped and linked to the previous one. Each digital record or transaction could be reorganized as a block which is linked to a specific participant. Essentially, all these blocks form a chain which cannot be altered and can only be updated with the approval of members.[26] Hence, the blockchain presents a true and verifiable record of each and every transaction ever made in the system. Hence, the blockchain presents a true and verifiable record of each and every transaction ever made in the system a secure messaging and transaction platform. Various militaries are found working towards using this technology in the arenas like military logistics, procurement and finance, project management and international collaborations.

3D Printing is a type of advanced manufacturing that are used to create three-dimensional structures out of plastics, metals, polymers, and other materials.[27] These constructs are added layer by layer in real time based on digital design. This technology facilitates the creation of very intricate and complex structures which are not possible with traditional manufacturing techniques. This is an

attractive technology for process improvement within the armed forces as itis cost-effective by quickly producing small replacement parts onsite instead of waiting for the supply chain to send equipment far off.[28]

For long, various industries both in civilian and defence sector are using the machines which are based on computer numerical control (CNC). Here during the production the machines execute preprogrammed sequence of control commands. There is a likely major disruption in this process where there products are produced batch wise in fixed quantities during every iteration. The process of Additive Manufacturing (AM, also known as 3D Printing) is a process that produces a project by deposing the materials layer by layer. Here for the development of any product a digital file first gets made (programmed) and the process of printing undertakes accordingly. Various digitally printed products are much lighter in weight (more than the 50% of actual weight) and could be produced in exact numbers as per the requirement (demand based). This technology is showing lot of promise and even the parts of aircraft and spacecraft are known to have been produced by defence industries.

Smart Factory is about "networking machines and systems by means of software so that intelligent communication with each other is made possible and the work steps can be automatically coordinated with each other." [29] Smart manufacturing is carried out in smart factories, using smart machines. These machines are characterized as "autonomous, flexible and adaptable" and are able to detect faults and even diagnose problems.[30] They can prolong their own life by undertaking health monitoring, taking timely preventive measures, optimizing maintenance schedules and increasing uptime as the requirement and capability of the entire system in use. Smart manufacturing utilizes the concepts of cyber-physical systems and various sensors, IT-based tools and applications and technologies like AI. Smart factories can offer defence industry an opportunity to develop technologically superior systems at lower costs.

Quantum technologies are expected to bring in major revolution to the technology domain. At present, states like the US, China, Britain, France and few others are found making major investments in this emerging domain of technology. These technologies if are expected to pose a challenge to the existing digital world and would change the existing notion of cyber security all together. Quantum cryptography, quantum communications and quantum computing are the important subsets of this technology where much work is happening. There is a significant interest of private industry towards undertaking research, development and innovation in this field of technology. The armed forces are expected to get greater advantage in arena like navigation since when fully developed these technologies would be challenging the existing

satellite based navigational systems.[31]

Going forward, the rapid advances in disruptive technologies would surely have a huge spillover effect on all domains of armed forces and specifically on warfare. It would not be wrong to say that the future battlefield might resemble a virtual video game battlefield where disruptive technologies would play a crucial role.

Military and the Future of War in the Age of Disruptive Technologies

The future battlefield is expected to be densely populated by a variety of entities (or things) —some could be intelligent, and some could be marginally so—performing a broad range of tasks like sensing, communicating and coordinating with each other and human war fighters. Some of such devices are also expected to take the decisions on the battlefield for their human masters. Such devices could include sensors, smart-munitions, weapon delivery platforms, vehicles, robotic systems and human-wearable devices. Their capabilities could vary and may include collecting and processing information, acting as agents to support sense making, undertaking coordinated defensive actions and 'releasing' a variety of effects on the adversary. In future battlefields, many of the functions would be performed collaboratively while continually communicating, coordinating, negotiating and jointly planning and executing their activities. In essence, these technologies could emerge not only as a force multipliers but they could have the potential to change the purpose and processed of war fighting.

For militaries, it is important to note that data analytics is not simply a quantitative increase in information, but a qualitative change offering some pinpointed solutions to undertake operational decisions. The processed data is often clear, actionable and updated in real time, which can facilitate smart decision making to minimize risks and interoperability. Working with data analytics in combination with other disruptive technologies imply seeking patterns and correlations that may not tell why something is happening, but rather alert that it is happening. New parameters can be deployed to attain real-time correlations and to ensure a more comprehensive early-warning system.[32]

Military performance is considered "superior" when their actions are backed by timely, specific and actionable intelligence. Also, specific processes coordinate their actions among themselves. In conventional and sub-conventional conflicts the tools used for border, maritime and space management can be used in operational planning to ensure better decision support tools as "visualization" platforms with real-time monitoring and enhanced situational

awareness. For instance, the introduction of Lethal Autonomous Weapons System (LAWS) on the battlefield. These weapons would not only open up a world of new capabilities but have also been predicted to outperform humans on all platforms. A defining feature of this weapon systems is precisely their ability to operate autonomously that is, once activated, they can select and engage targets without further human intervention.[33] AWS can take many different forms, from singular entities to swarms, and they can operate on land, in air, and at sea. While many of the systems so far have mainly designed for defensive, surveillance, or reconnaissance purposes, and have a varying degree of autonomy. Nonetheless, developments are underway towards building more lethal and offensive systems.

Internet connected devices could automate many monitoring, management and repair tasks that currently require human labour. Indeed, the cross-section of the IoT, analytics and AI would create a "global network of smart machines" that conduct an enormous amount of critical work. For instance, these technologies can also be used in inventory management and supply chain management for the supply of arms and ammunition. IoT in military domain covers a wide gamut of applications to support tactical reconnaissance, smart city monitoring and leveraging services in smart city environments for disaster support. Facilitating interoperability and integration of disparate technologies.[34]

Disruptive technologies are also known to augment cyber security. Integrating Machine Learning and Artificial Intelligence into the breach and threat analysis capacity allows generating and spreading response faster than a human would react. In addition, storing information of previous incidents shortens predicting the potential threats and aid to develop strong and secure protection against them in the future. To reduce cyber threats and hacking, organizations maintain data confidentiality, integrity and availability across the infrastructure. Mechanism or methods for secure communication, storage and sharing of data should be implemented including the use of the latest cryptographic methods or security algorithms. Transparency and data security by design is needed.

Many of these technologies also find applications in detecting chemical and biological warfare agents or help map the quickly spreading pandemics. In the Western part of Africa, several states are recording data related to previous disease outbreaks, such as Ebola, to predict where an infection may begin, what may cause its spread and identify high risk zones which can be targeted with prevention programs.[35] Even today, the rapid spread of the Corona Virus (Covid-19) is being tracked and monitored by the cross section of various disruptive technologies.[36] The association of AI and blockchain is expected to create various possible applications for civil and defence fields.

Humanitarian Aid and Disaster Relief (HADR) operations is another arena where countries can pool together their knowledge and expertise to help another. For instance, Japan which more often has to face the wrath of range of natural disasters from hurricanes to earthquakes (even Tsunami) and now has become an expert in addressing the issue effectively. With the rise in cases of natural disasters across the world, Japan can lend its expertise to ensure preventive measure.

Disruptive technologies could help nations prepare better for both manmade (artificial) and natural threats by undertaking environmental modelling, pattern analysis and social network analysis. As such the statistical techniques like predictive analytics include data modeling, machine learning, AI, deep learning algorithms and data mining. All this could help to model the possible security challenges. It is important to note that in the battlefield of tomorrow the adversaries would also have access to various the disruptive technologies. Hence, there would be a necessity to quickly develop the counter and counter-counter mechanisms. In a defensive mode the military focus on such technologies should be such they should be effectively used for limiting damage and preventing the escalation of conflict.

Future of Disruptive technologies

For the predictable future, it has been forecasted that countries may fight over a new resource called “data.” Additionally, the nations with more data and better AI systems would be better positioned to reap the greater benefits for their security architecture. There would be both the advantages as well as risks in using such disruptive technologies. Such technologies could create challenges for national practices, especially with regard to privacy and state security, which can lead to “data nationalism.”Governments and economic entities could centralize the collection and analysis of regional and global data. Particularly, with the defence related data there could more problems. On various occasions the secrecy aspect would restrict data availability. This could lead the systems to work on very limited and old data-sets. Possibly, since the systems data dependent the limited data would impact the quality of output. In addition, the adversaries would give more thirst to ensure data espionage. In addition, there could be issues of spurious data too.

Data security will become a major concern for organizations as, without a strong security architecture, massive amounts of data flowing and stored across the networks would be exposed to vulnerabilities. This fear ties closely with the

rise of the internet as a 'fake news' engine, leading people to make unwise decisions under the influence of 'junk information.' Data quality would be a huge issues. Market would be full of incomplete, inaccurate and irrelevant data. Military establishments would be required to evolve multilayered structures for data management. Present level of AI may not sufficient to address all such challenges. Significant amount of investments would be required to be made to develop new software tools and more importantly there is a need for a leapfrog in the technology of AI.

The projected technology disruption is not only expected to change the methods of war fighting but could even revolutionize the concept of future warfare. At present, there has been a rudimentary display of ideas by strategists about how these technologies could be employed as instruments of war fighting. It would take some more time to completely assimilate these technologies in the defence architectures of nation states. It would impact all forms of warfare from conventional to nuclear. States with a technological edge and financial capabilities and the ones which have already established technically superior military structures have already begun to imbibe disruptive technologies in some form of the other. Maturing of these technologies would force the state to make relevant changes in their war fighting doctrines too.

Since many of the disruptive technologies are dual use in nature and hence find significant relevance in the civilian sector. Some of them have already evolved in the civilian/commercial domain, to a certain extent. Military strategists can, therefore, assess and scrutinize their innovation models and develop military-specific versions of them. Subsequently, they can encapsulate these technologies within their security architecture as per their suitability and need.

Today, there is barely any country that has remained untouched by the rapid advances in disruptive technologies. However, the formation of global agreements and decision making is still continuing at a snails' pace. Most of these technologies have the potential to challenge the existing force structure of the nation-states. Obviously, both inter and intra service turf wars could also have some influence on adopting to such technologies. Various defence industry related challenges of the present like covert technology transfer, international cartels, middlemen, black markets, money laundering and monetary manipulation are likely to exist in some form or other. Effective regulation of these technologies would be a challenge because of their nature and inherent dual-use capabilities. There also exists a likelihood that these technologies could eventually facilitate an arms race (partially, since it has already begun). The arms race is not in the interest of anyone and therefore

requires like-minded states and organisations to be proactive in regard to the formulation of regulative bodies for these technologies and ensure that the entire process remains dynamic and transparent since these technologies are expected evolve continuously.

Although, most of technologies discussed are still in the process of evolution, but nevertheless they are expected to provide innovative, real-time, and more granular insight for myriad defence and civil applications. Obviously, the opportunities for individual countries will remain unequal and will depend on the state's overall technology setup. Also, the military industrial complex should be capable of fast adaption to such disruption. More importantly, the vested interests of major defence equipment design and manufacturing industries would also play a major role towards acceptance of new technologies. The availability and accessibility of the networks for generating data would also play a major role. On the whole, disruptive technologies are ordained to generate new solutions and opportunities that will have a long-lasting impact across the sectors.

References

1) *Yi-Ting Chen and Edward W. Sun, "Automated Business Analytics for Artificial Intelligence in Big Data @X 4.0 Era" in Matthias Dehmer and Frank Emmert-Streib (ed), Frontiers in Data Science, (CRC Press, New York: 2018), p. 224.*

2) *LI Guoping, Hou Yun and Wu Aizhi, "Fourth Industrial Revolution: Technological Drivers, Impacts and Coping Methods," (Springer, 2017: China), v. 27, n. 4, pp. 626–637.*

3) *"Moore's Law," see http://www.mooreslaw.org/,accessed on Jun 28, 2022.*

4) *M K Sharma, "Cyber Warfare and National Security," (KW Publishers, New Delhi, 2018), pp. 206-208.*

5) *Roland Heickero, "Cyber Security challenges for Asia in a 2030 Time Frame"in "Imagining Asia in 2030: Trends, Scenarios and Alternatives."*

6) *Mike Kavis, "Forget Big Data -- Small Data Is Driving The Internet Of Things", Feb 25, 2015, https://www.forbes.com/sites/mikekavis/2015/02/25/forget-big-data-small-data-is-driving-the-internet-of-things/#1f0afa9c5d7e, accessed on March 19, 2022.*

7) *S. Maital and D.V.R. Seshadri, "Innovation Management," (New Delhi: Sage, 2012), v. 29.*

8) *Greg Satell, "How to Manage Innovation," Forbes, March 7, 2013, see https://www.forbes.com/sites/gregsatell/2013/03/07/how-to-manage-innovation-2/#7f09d0b24785 accessed on 16 Jun 2022.*

9) *Ajey Lele, "Disruptive Technologies for the Militaries," (New Delhi: Springer, 2019), v. 132.*

10) *Howard M. Shore, "Is there a Difference Between Innovation and Disruption," see Activate Group Inc., September 14, 2015, see https://www.activategroupinc.com/2015/09/is-there-a-difference-between-innovation-anddisruption/accessed on 16 September 2019 and https://www.open.edu/openlearn/mod/oucontent/view.php?id=3440&printable=1, accessed on Jun28, 2022*

11) *Chris Price, "The power of disruption and the struggle for businesses to scale up," The Telegraph, April 1, 2019, see https://www.telegraph.co.uk/business/advance-series-event/power-of-disruption/accessed on 17 September 2021.*

12) *"Power of data for business disruption" The Economic Times, July 11, 2019 see https://cio.economictimes.indiatimes.com/news/corporate-news/power-of-data-for-business-disruption/70155597accessed on 17 September 2021.*

13) *Abhishek Narain Singh, "Power of Data," The Smart Manager, November 23. 2018, see http://www.thesmartmanager.com/technology/power-of-data.htmlaccessed on 18 September 2020.*

14) *Nick Couldry and Ullses A. Mejias, "The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism," (New York: Stanford University Press, 2019).*

15) *Ibid.*

16) *Osama Manzar, "What is Data Colonisation and Why it Matters to us in India," Business Standard, August 17, 2017, see https://www.business-standard.com/article/economy-policy/who-owns-your-data-india-needs-to-tackle-data-colonisation-soon-117081700234_1.htmlaccessed on 18 September 2019.*

17) *Alan Marcus, "Data and the fourth industrial revolution," World Economic Forum, December 02, 2015, see https://www.weforum.org/agenda/2015/12/data-and-the-fourth-industrial-revolution/ accessed on 18 September 2019.*

18) *"The Keys to Data Protection," August 2018, see https://privacyinternational.org/sites/default/files/218-09/Data%20Protection%20COMPLETE.pdf accessed on 18 September 2019.*

19) *Big Data: What it is and Why it matters? SAS, See https://www.sas.com/en_us/insights/big-data/what-is-big-data.htmlaccessed on 18 September 2019.*

20) *Jacob Metcalf, Emily F. Keller and Danah Boyd, " Perspectives on Big Data, Ethics and Society,"The Council for Big Data, ethics and Society, May 23, 2016, see https://bdes.datasociety.net/council-output/perspectives-on-big-data-ethics-and-society/ accessed on 19 September 2019.*

21) *https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/accessed on 19 September 2019.*

22) *R. Minerva., A. Biru and D. Rotondi, "Towards a Definition of the Internet of Things (IoT)," in: IEEE Internet Initiative, see iot.ieee.orgaccessed on 19 September 2021.*

23) *Germany: Industrie 4.0, report prepared for the European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs: 5*

24) *Anupam Guha, "Who wields AI, and How," The Indian Express, 12 September 2017, see website indianexpress.com/article/opinion/columns/artificial-intelligence-can-become-an-emancipatory-agent-for-the-workforce-4839128/ accessed on 4 March 2020.*

25) *Dallas A. Powell, The Military Applications of Cloud Computing Technologies, US Army (USA), 2015 see www.dtic.mil/get-tr-doc/pdf?AD=ADA589625 accessed on 14 Feb 2020.*

26) *L. Mearian, "What is blockchain? The most disruptive tech in decades," May 21, 2018, http://computerworld.in/feature/what-blockchain-most-disruptive-tech-decades, accessed on March 1, 2020.*

27) *Berman, Barry, "3-D Printing: The New Industrial Revolution," Business Horizons, v. 55, n. 2, 2012, pp. 155–162.*

28) *Ben Werner, "Better Logistics, 3D Printing Will Quickly Return Navy and Marine Corps Aircraft to Service," U.S. Naval Institute News, October 8, 2018, see https://news.usni.org/2018/10/08/37127 accessed on 4 March 2020.*

29) *Frank Herrmann, "The Smart Factory and Its Risks," Systems, October, 10, 2018, v. 6.*

30) *R. McCormick and D. Hartmann, "Smart Factories Need Smart Machine," 2018, https://www.mouser.com/pdfdocs/ADI_Smart_Factories_Need_Smart_Machines.PDFaccessed on 4 March 2020.*

31) *Ajey Lele, Quantum Technologies and Military Strategy, Springer Nature, Switzerland, 2021*

32) *How Big Data Can Help The Developing World Beat Poverty, DataFloqsee https://datafloq.com/read/big-data-developing-world-beat-poverty/168accessed on 19 Jun 2022.*

33) *Ingvild Bode and Hendrik Huelss, "Autonomous weapons systems and changing norms in international relations,"RIS, Review of International Studies, v. 44.*

34) *Margaret Rouse, "Internet of Things," TechTarget, July 2016, see, http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT accessed on 20 September 2019.*

35) *Nita Bhalla, "Poor nations need help to use big data to tackle disease, poverty: expert," Reuters, July 10, 2017, see https://www.reuters.com/article/us-india-technology-development/poor-nations-need-help-to-use-big-data-to-tackle-disease-poverty-expert-idUSKBN19V0UOaccessed on 19 September 2019.*

36) *Iva Watson and Sophie Jeong, "Coronavirus mobile apps are surging in popularity in South Korea," CNN Business, February 28, 2020, see https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html accessed on 3 March 2020.*

ABOUT THE AUTHOR

DR. AJEY LELE

Dr Ajey Lele, is presently working as a Consultant with the Manohar Parrikar -Institute for Defence Studies and Analyses (MP-IDSA), New Delhi. He started his professional career as an officer in the Indian Air Force (IAF) but took early retirement from IAF to pursue academics. He holds a rank of Group Captain. His areas of research include issues related to WMD, Strategic Technologies and Space Security. He has widely published in these fields.

STRATEGIC ASPECTS OF COUNTERING 2.5 FRONT WAR

BY BRIG HH MAHAJAN

It is 2022.India's economy is poised for high growth in its 75th year of independence. China and Pakistan have serioussecurity,economic and domestic problems. They may decide to collude against India and start war.

A victory over India in a carefully planned, limited war, would hurt the Indian government enough to lose aelection and bring in a government more amenable to make concessions on border issue,trade and Kashmir.

While facing the possibility of a collusive two-front attack by China and Pakistan, the Indian armed forces have to deal with the 0.5 front of internal terrorists, saboteurs and collaborators

The term "two and a half front war" pertains to the Indian armed forces preparing to simultaneously fight conventional wars to the North and West, while also battling any insurgency that might be ongoing at that time in the hinterland, having to battle internal enemies.

Given the significant costs of engaging India in combat, and the growing range of indirect and non-military tools at their disposal, both Pakistan and China are seeking ways to achieve relative gains without triggering escalation. From fake news and online troll farms to terrorist financing and paramilitary provocations, these approaches often lie in the contested arena somewhere between routine statecraft and open warfare – the "grey zone".

What is 2.5 front war and its likely implications on India's security framework. Will the challenges from China and Pakistan, their collusion to tie down India's army along the eastern and western fronts succeed?What efforts have been taken uptill now and is security doctrine of the Modi government ready to meet the challenges of 2.5 Front War?.In this article following aspects will be covered:-

- Security Doctrine 2.5 Front War
- Likely Contingencies Leading to 2.5 Front war
- India's Counter &Conductof 2.5 Front War

- Role IAF, Navy in 2.5 front war
- Time Frame For 2.5 Front War and Use of Nuclear Option
- Additional 'Half-Front' More Dangerous
- Cyber and Space Domain
- What Else should be done?
- Forge Partnerships With Global Powers
- Making China and Pakistan fight 2.5 front war

Security Doctrine 2.5 Front War

India's primary goal if confronted by a China-Pak collusive attack should be to destroy Pakistan as a viable entity and hold China to a draw through an offensive-defence strategy. No matter what the outcome of the war, Pakistan should never ever have the capacity to conduct war against India.

General V. K. Singh, referred to Pakistan and China as "two irritants" in October 2010, and indicated that the armed forces were preparing for a contingency in which they might have to confront China and Pakistan simultaneously.

In September 2020, Chief of Defence Staff(CDS) General Bipin Rawat acknowledged, "Chinese continued military, economic and diplomatic support poses the threat of coordinated action along the northern and western fronts, which we have to consider in our defence planning. India is ready for a 'two-and-a-half front war', CDS General Bipin Rawat had said referring to Pakistan, China and the internal conflicts.

At his annual press conference held on 12 January 2022, army chief General M.M. Naravane outlined that an active 'two and a half front war is now a reality. The two fronts being China and Pakistan and the half front being counter insurgency."There is increased cooperation between Pakistan and China, both in military and non-military fields.

How ever much has changed in terms of our capabilities. The Army, Navy and IAF are now very much prepared for 2.5 front war. These remarks are reassuring messages from the top military leadership.

Likely Contingencies Leading to 2.5 Front war

Various contingencies for start of war could be as under:-

- China and Pakistan could collude to launch a surprise-coordinated attack

from both India's north and west.

- Or China could engage in strategic opportunism in an India-Pakistan conventional military engagement.
- A variation of that could be a scenario in which a significant conventional conflict between India and Pakistan threatens CPEC assets and Chinese citizens in Pakistan, giving China motivation to distract India by starting a separate conflict along the LAC.
- Another variation could be the use of Chinese naval power to divert and distract the Indian Navy's efforts to blockade Pakistani ports as part of its coercive strategy.
- Pakistan could take advantage of an India-China conflict to mobilize its military against India.
- China can take on India directly, militarily without Pakistani assistance. But its hand could be forced for geostrategic reasons, such as sending a message to other smaller countries in the region.
- In a border war between India and China that Pakistan could exploit to open a front across Kashmir to compensate for its disadvantages versus India.
- Short of joining a war, even a military mobilization by Pakistan could tie up Indian troops on that front. This was not done by Pakistan during the Ladakh border crisis between India and China, a fact acknowledged by Indian Armed Forces leadership.
- An armed conflict with China is most likely to lead to India facing a 2.5 front war scenario, drawing in Pakistan either of its own or under Beijing's pressure.

India's Counter to 2.5 Front War

The Indian Armed Forces plan for dealing with a 2.5 front conflict revolves around identification of a primary and a secondary front.

In January 2020, General M. M. Naravane reiterated that in the case of a simultaneous 2.5 front threat on the country's northern and western borders, there would be a primary front and a secondary front: "Most of our aggression will be concentrated on the primary front and we will adopt more deterrent posturing on secondary front.

We have formations which can quickly be moved from the east to west or vice-versa. In this manner, we will be able to deal with both fronts to ensure

territorial integrity is not compromised.

Indian strategy in case of a 2.5 front war will be as under:-

- No territorial loss is acceptable on either front.
- The Indian Armed Forces would assume a more offensive posture against one adversary (China) while holding the defenses, and a simultaneous threat of limited military punishment against the other (Pakistan) to prevent a loss of territory. Deterrence means ,India will prevent Pakistan from initiating a 2.5 front threat by means of threat of reprisal.

After the 2020 Ladakh border crisis, the Indian Army has initiated a rebalancing strategy, under which it has moved troops from the Pakistan front against China. It has converted one of the three existing strike corps (offensive fighting formations launched in enemy territory) meant to operate along Pakistan into a China-facing mountain strike corps. This will give the army two mountain strike corps against China, one in Ladakh and another in Arunachal Pradesh.

In January 2020, Gen Naravane said that Siachen and Shaksgam Valley are the places where territory of these two countries meets. Therefore, it is important to be on guard and keep that area in our possession." This is the area where the Ladakh border crisis with China occurred in 2020, and the standoff remains unresolved.

Conduct of 2.5 Front War

How would a 2.5 front war play out? The war would be launched by China at a time and place of its choosing. China's People's Liberation Army (PLA), after mobilizing its forces into Tibet, activating its airbases, deploying missiles, and moving its navy into the Indian Ocean, could limit the conflict to only one theater, say Ladakh, or could undertake conflict all along the LAC.

Pakistan would have the option to enter such a war simultaneously, or could choose to commit itself militarily only when India appeared to be under severe military pressure. Depending on the progress of PLA operations in the Daulat Beg Oldi sector , military collusion in the Karakoram Pass region is considered the most likely scenario.

Following the lessons learned from Operation Parakram in 2001,India settled on a proactive strategy against Pakistan, called as the Cold Start strategy. It has led to reduced mobilization timings and the placement of formations closer to the border, and envisages the employment of forces across the border for

quick gains before the strike corps come into play.

The additional reserves and the Mountain Strike Corps have given the Indian Army additional depth in its defenses as well as a capability to undertake a counteroffensive across the LAC.

The Chinese front will become the primary front . Without a 2.5 front war, India could respond to Pakistani moves in J&K by opening up along the international border with its strike corps.

Even though the government directive is to prepare for the expenditure of ammunition at 30 days at intense rates and 60 days at normal rates — a total of 40 days at intense rates — the government took a decision in 2016 to stock only 10 days of ammunition to fight a war against Pakistan.

In 2019, General BipinRawat confirmed that he had focused on building up stocks for a 10-day war, and a war against China would need ammunition for 30 days of intense warfighting.

He also mentioned that arms and ammunition could be easily moved from one front to another if a threat developed on the China front.

Role For IAF, Navy in 2.5 front war

The IAF would execute a parallel strategy, and has ability to dominate the Pakistan Air Force.

The IAF has only 30 squadrons of fighter aircraft while it requires at least 45 combat squadrons .In last IAF training exercise, Gagan Shakti, in 2018, the IAF demonstrated its capability and reinforced its concept of tackling a 2.5 front war.

With its overwhelming superiority over Pakistani Navy, the Indian Navy would play an important coercive role in making its effect felt on ground operations.

India has naval dominance in the Indian Ocean over the sea lines of communication that carry a majority of China's trade. Neither China nor Pakistan can seriously threaten India's maintenance axes.

The Indian Army would be closely supported by the Indian Air Force and the Indian Navy; the latter could put the PLA Navy under pressure in Malacca Strait.

Time Frame For 2.5 Front War

Even though the government directive mandates the armed forces to be prepared for a war for 40 days of intense warfighting, it may be a shorter war with both adversaries. India envisages an international intervention in a short period of time in a military conflict with China, Pakistan and hopes for early gains to hold good on the negotiating table before nuclear weapons come into play.

However the Ukraine war lessons of much longer war will have to be studied and directive corrected accordingly.

Use of Nuclear Option

India has promised a rethink on its No First Use policy for use of nuclear weapons .In case the lack of conventional superiority with the Indian Armed Forces creates a scenario where the loss of territory to China is imminent, India could be forced to threaten the use of the nuclear option against China/ Pakistan as deterrence. The redline for India's threat of using the nuclear weapons could be different in the case of Siachen, Kashmir, and elsewhere .

Pakistan will always threaten use of tactical nuclear weapons (TNW) to neutralize India's conventional superiority and try to halt India in its tracks.

We could use similar tactics against China when vital areas like Siliguri Corridor is threatened.

However use of many highly destructive weapons such as Mother of all bombs or Vacuum bombs should be considered as is being done in Ukraine war.

However India should continue to modernize its Nuclear Triade for implementing nuclear option.

Additional 'Half-Front' (Kashmir, Maoists Areas, Insurgency In North East, Illegal BanglaDeshi Migration) More Dangerous

The grey zone phenomenon is also referred to as hybrid threats, sharp power, political warfare, malign influence, irregular warfare, and modern deterrence. Although it reflects an age-old approach, it is newly broad in its application. Today, the toolkit for coercion below the level of direct warfare includes information operations, political coercion, economic coercion, cyber operations, proxy support, and provocation by state-controlled Forces."

China, has implemented a well orchestrated campaign approved and controlled by the highest levels of the Chinese Communist Party and the People's Liberation Army. Grey zone actions are not those of tactical commanders freelancing. They are purposefully constructed to side-step military escalation – crafted as a form of carefully scripted brinkmanship."

China Is the "largest country undertaking grey zone actions". Whether in the South China Sea, the East China Sea or on its border with India, China has employed innovative and imaginative grey zone tactics in its quest for a persistent strategic advantage over others.

Pakistan has learned well from China .

But it cannot survive treason from within

Pakistan has been able to radicalize the Kashmir valley and create a limited civil unrest and a situation of hybrid conflict there. Low level terror acts will continue.

India has, therefore, to continue to stabilise the situation in J&K through a combination of military means and good governance. This necessitates heavy commitment of troops and, hence, can be termed as 'Half Front'.

Terrorism in Kashmir valley is at all time low.

Tackling Kashmir valley terror, will be passed on to the Central Reserve Police Force to keep rear areas secure during war.This is well within their capability.

Insurgency in the north east India is at all time low, however China will make all out effort to start it again. Intelligence based operations have to be carried out regularly to end it.

The CAPF aided by local police will take on the insurgency during war and manage the Myanmar border. The Assam Rifle can reinforce our defences against China releasing deployed formations for counter attacks or counter offensive in Arunachal and Sikkim.

Maoist control a large part of Central India. This insurgency is away from both China and Pakistan border. It however is a big threat to India's security. The central armed police forces have to carry out aggressive operations to break the back of armed Maoist.

India's security forces are well placed to tackle terrorism or counter-insurgency. But it is equally important to neutralize elements in India sympathizing with Pak-China.

India is actually battling some of its own citizens the internal subversives who happen to be the most diabolical , because they are indistinguishable

from the masses and so escape scrutiny. The faceless fifth columnists and homegrown inimical elements are now peddling the cause of hostile neighbours with even greater energy and destabilizing the system is their paramount goal. Their morbid reliance on social media forums as a tool to vilify the republic, institutions and individuals has degenerated into a deadly hybrid warfare.

They will have to be tackled with the help of other instruments of nation such as NIA,CBI,NTRO,ED,Economic Intelligence Agencies etc

Cyber and Space Domains

Rising cyber threats, especially from China, and its growing Intelligence Surveillance Reconnaissance (ISR), aerospace, artificial intelligence and unmanned weapon systems will add another critical dimension to their capabilities.

India has to develop its own capabilities both defensive and offensive in this field over and above its full preparation for conventional war.

Tremendous help Is being given by USA and Europe for conduct of Information and psychological war which Ukraine seems to be winning .High quality technical intelligence provided by the USA to Ukraine has resulted in destruction of many important military targets .

India could expect similar help from the western countries.

Implications of a Two or Two and a Half-Fronts War

(a) Vast geographical separation makes rapid movement of large quantum of troops from one sector to another, not only for the Army but also for the Air Force challenging. This results in separation of forces. Higher level of inter-theatre mobility will enhance operational options is being created, which has to be expedited.

(c) Navy will have to be divided into the Arabian Sea and the Bay of Bengal.

(d) A war on two fronts will also result in much higher degree of ammunition consumption and thus much higher stocks of ammunition and spares need to be available ‘abinitio’.

What Else should be Done?

Indian Armed Forces, will fight with weapons that they have and They will fight to the very best of their capabilities. They have made suitable plans to optimize their potential in every scenario.

However, it is better for the country to be aware of the actual situation, and for that they need to be guided by the Army Vice Chief's presentation to the 'Parliamentary Committee for Defence'. Briefly, it states that large per cent of the arsenal requires up gradation ,modernization and making up of deficiencies and operational voids.

India need to divide our preparation based on twin approaches of what needs to be done in immediate future (not more than 2-3 years) and what all must be achieved in next 5-7 years (mid-term).

- Minimum serviceability rate for all types of equipment and armament must be maintained at a readiness level of minimum 70 per cent at all times. For this the assistance of our indigenised companies in the Defence Industrial Base should be taken as a permanent measure.
- Refining the Higher DefenceOrganisation and Inculcating Joint-ness amongst Armed Forces. Appointment of CDS and theatre command is the way ahead.
- Budgetary Allocations most important issue.Much enhanced allocation of budget is a pre-requisite to attain preparedness and thus security. This will have to be done for a long period. Budgetary allocations need to be increased to 3 per cent of the GDP.
- Defence Industrial Base to be strengthened, and 'Make in India' – to be given a push.

Forge Partnerships With Global Powers

To overcome its power deficit when confronted with a 2.5 front challenge, India must forge partnerships with global powers especially the United States. Prime Minister Shree Narendra Modi attended the summit of the Quadrilateral Security Dialogue, with his counterparts from the U.S., Australia, and Japan. China, figured prominently in the discussion. During the Ladakh standoff, USA had provided "some information, cold-weather clothing, some equipment."

The USA and Europe supplied Ukraine with limitless quantity of arms and ammunition. Technical intelligence support has been of very high quality. Similar help should be expected & must be demanded by India.

Long-standing military and strategic relationship with U.S. is required where cooperation, support, and technology transfer are routine activities to counter China. Proactive diplomacy for building alliances is the way forward.

Making China and Pakistan fight 2.5 front war

All the while we keep on talking about India having to fight a 2.5 front war. Is it possible for India to make China fight a 2.5 front war? Yes it is definitely possible. Can we take help of Quad countries especially Japan,USA ,Vietnam to confine Chinese Navy in the South China Sea? is it possible to open up another front against China with the help of South Vietnam on the land border? is it possible to activate Tibet hinterland with the help of own Special Frontier Force and Tibetan government in exile so that Chinese army cannot fight effective war on the line of actual control. Can unrest be created in China's xinjiang province and Mongolian province with the help of Uighurs Muslims and Mongolia population against the Chinese.

Is it possible to take help from Pak opposing groups such as Balochistan Liberation Army to target China Pakistan economic corridor?

It must be understood that the Chinese soldiers are not 7.5 feet tall. China and Pakistan can also be made to fight on 2.5 front war. We should not restrict ourselves to defensive operations while fighting a 2.5 front war but also think of carrying out offensive operations to make China fight a 2.5 front war. There are a large number of ways it can be done except that we should have the willpower to make China pay for their aggression.

Conclusion

This hybrid war is a bigger challenge than conventional war and requires whole govt approach and would be a separate topic for an article.

It is time to drop this soft approach. India must accept the truth that the country' self-interests and security are above all else. Eliminating internal enemies should be a primary task. This will involve tracking down suspected treasonable individuals and groups, infiltrating and manipulating them. This strategy is especially necessary against the urban Naxals, terrorists supporters who have grown roots in India's colleges and universities and are poisoning young minds against the nation and its values. Indians in the pay of foreign intelligence agencies can be identified using technology and human intelligence

More dangerous individuals – such as terrorists and those who encouraged, trained and supported them should be eliminated.

India will almost certainly be fighting on 2.5 fronts. To prepare for such an eventuality, apart from beefing up its offensive capabilities, India needs to change its war doctrines, including its nuclear doctrine, to deter the enemies.

As far as the three Services are concerned they must try and ensure that the allotted resources are optimally utilised and joint-ness is implemented in letter and spirit. India has to be prepared to fight wars with due emphasis on Cyber and Space dimensions without sacrificing our capabilities for conventional warfare. But it is quite clear that the Armed Forces are quite capable of meeting the 2.5 front challenge head on.

END NOTES

- *https://www.youtube.com/watch?v=zNfP8h6gRXg*
- *https://www.youtube.com/watch?v=N1QB1f-L5Bs*
- *https://www.youtube.com/watch?v=iH-oK6GFoMY*
- *https://www.news18.com/news/india/india-ready-for-two-and-a-half-front-war-says-army-chief-1426427.html*
- *https://www.indiatoday.in/magazine/up-front/story/20210125-the-two-and-a-half-front-war-1759580-2021-01-17*
- *https://www.hindustantimes.com/opinion/the-threat-of-india-s-two-and-a-half-front-war-101641647815971.html*
- *https://organiser.org/2022/06/09/85009/bharat/the-two-and-a-half-front-war/*
- *https://www.nationalheraldindia.com/opinion/not-ready-for-two-and-a-half-front-war*
- *https://www.quora.com/In-the-military-terminology-what-does-a-two-and-a-half-front-war-mean*
- *https://www.thehindu.com/news/national/army-prepared-for-two-and-a-half-front-war-gen-rawat/article18867921.ece*
- *https://en.wikipedia.org/wiki/Two-front_war*
- *https://www.nriherald.com/post/bipinrawat-2-5frontwar-nriherald-australia*
- *https://idsa.in/askanexpert/two-and-a-half-front-war-india-prepared-for-it*
- *https://indianexpress.com/article/india/indian-army-prepared-for-a-two-and-a-half-front-war-army-chief-general-bipin-rawat-4694292/*
- *https://www.theweek.in/news/india/2020/01/11/how-will-india-handle-a-two-front-war-army-chief-general-naravane-explains.html*
- *https://www.oneindia.com/india/with-threats-from-2-5-fronts-govt-may-go-for-deep-dive-on-appointment-of-new-cds-3345426.html*

ABOUT THE AUTHOR

BRIG
HEMANT MAHAJAN

Brig Hemant Mahajan is a prolific writer and speaker on all aspects of National Security. He is M Sc., M Phil in Defence Studies. He joined IMA Dehradun in July 1973 and passed out as a Commissioned Officer on 15 June 1975.He has served extensively in Counter Insurgency Operations in Jammu & Kashmir, Punjab and North East and has taken part in all important operations undertaken by the Army since 1975 till 31 Jan 2009. He has been appointed as independent member of security commission of Union Territory Div, Daman, Dadra, Nagar Haveli for two years

A TALE OF TWO BUFFERS

BY JAYANT UMRANIKAR

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us,…….

'A Tale of Two Cities'

Charles Dickens

Dickens was describing times in two cities, London and Paris during the French Revolution, but the description fits the buffer states, caught between two rival nations. They have everything, they have nothing.

Buffer States

As per the theory,states do not choose to become buffers but this role is thrust upon them by a hostile international environment over which they have no control. Buffer states are lesser entities sandwiched between more powerfully endowed, ambitious, and often aggressive states.[1] The role of the buffer state is assigned by these external competitors to become sacrificial lamb in a larger contest. Their national interests are ignored or treated with disdain by the greater states who set the dimensions and lay down the guidelines of confrontation. A buffer state has to live with diminishing sovereignty, accept that its national destiny is influenced externally.Its territorial integrity is neither fully respected nor legally protected by neighbours. 'Buffer states are extensions of balances of power, not international law.' As such, they are protected by military-political conditions, not moral-legal procedures. If their status as buffer states is respected, their tenuous existence is sustainable. Yet, if the pattern of regional relationships changes significantly, buffer states have to pay the price for temporary larger power equilibrium, which may vary between a national humiliation and even extinction.

Mandala: Arya Chanakya (4th Century BCE) had evolved Mandala (Sphere of influence) Theory and advocated using'Six Policies', including use of a buffer:

Sandhi: Peace based on the "Pledges" by both the nations.

Vigraha: Offensive operation or war.

Yana: Moving the army against the enemy or deploying along the border.

Asana: Indifference or Neutrality

Dvaidhbhava: Dual policy; Keeping peace with one nation but waging war with another.

Samashraya: Alliance (Friendly ties); a stronger state in order to protect itself from an equal rival power uses an adjacent weaker state in alliance, as a shield (buffer) to defend itself from potential rival.

The 'Ring Fence':

The British rulers in India had adopted foreign policy known as the 'ring fence',directed towards securing the alliance, integrity or neutralization of the borderlands and minor states lying on the land approaches to the Indian Empire. The system had two, more or less, concentric circles. 'The inner ring consisted of the Himalayan kingdoms of Nepal, Bhutan, Sikkim,the tribal areas in North/Northeast Assam and on the Northwest Frontier. The outer ring consisted of the Persian Gulf sheikhdoms, Persia [Iran], Afghanistan, Tibet and Siam. The inner ring was gradually brought under varying forms of control, while intensive diplomatic activity, backed by the threat or use of force, denied a foothold in any of the buffer states in the outer ring to a major power without compensating advantage.' [2]

Afghanistan

The British colonial office anticipated the Russian quest for the warm waters of the Indian Ocean.They sought containment of Russian forces in Central Asia, to the north of the Oxus (Amu Darya) River. Thus, Afghanistan became a classic buffer state between its two powerful neighbours. Besides, Britain developed 'Forward Policy' of stationing of the British-Indian contingents in Afghanistan and subordination of Kabul rulers to British diktat. This led to the Anglo-Afghan War (1838-1842). Thereafter Kabul treated Britain as its primary enemy and,after the British withdrawal, invited Tsarist emissaries

to Kabul.This started the Second Afghan War (1878) in which the Afghan leader, Sher Ali, sought refuge in Russia after the British occupied Kabul. The British had to decide on either annexing Afghanistan or installing a 'friendly' government that would ensure the security of India and the Persian Gulf. After the first war London had assured the Afghans not to interfere in their internal affairs.Besides, the permanent garrisoning of Afghanistan against hostile Afghans would deplete treasury and their limited forces, weakening their hold over India. The British, therefore, opted for Afghanistan as a buffer state and restricted its relations with other governments.To ensure its 'neutrality,' they installed Sardar Abdur Rahman in Kabul, due to his loyalty to the British Crown.They continued to maintain a strong garrison in Kandahar.

Afghanistan ceased to be a buffer for India as Pakistan emerged on the west after partition. However independent India inherited another buffer, Tibet.

Let us examine the comparative tale of two buffers, Tibet in the Indian Subcontinent and Ukraine in Europe.

Tibet

Through the eighteenth and nineteenth centuries, British empire in India kept expanding to the east till it reached the Himalayas and inter alia,Tibet. Historically, Tibet has been autonomous. China had some control over Tibet, Nepal, Sikkim and Bhutan as their rulers paid tribute to China and held Chinese official rank. When Mongols conquered Tibet (thirteenth century) Tibetan Lamas evolved an arrangement with them known as Cho Yon or Patron-Priest relationship.

After the First Anglo-Sikh War, under Article 4 of the Treaty of Lahore (March 9, 1846), the Sikhs ceded all territories between Rivers Beas and Indus to the British; Article 12 gave Gulab Singh 'Independent Sovereignty" of these territories. This arrangement was sanctified through Article 1 of the Treaty of Amritsar (16 March, 1846) and its Article 4 added that the territories of Gulab Singh shall not be changed without British concurrence. They included Karakoram in the north and its extension south-east.

Johnson, an official of the Survey of India, in 1865 drew the "advanced boundary line of the Kashmir State that extended the ceded territories of the Sikh Empire eastwards to the Kun-Lun watershed encompassing Aksai Chin, projected in the Survey of India map of 1868 and continued to be shown as such thereafter. In 1872, Johnson joined the Kashmir Maharaja's service as Wazir of Ladakh;possibly a return-favour for cartographically extending the

Kashmir State domain.

In 1893, the Chinese official at Kashgar handed a map to the local British consul-general,McCartney, showing the proposed boundary along the Karakoram Mountains, which was a natural boundary stretching the border up to the Indus-river watershed.

This line, called the McCartney-MacDonald Line, was presented to the Chinese in 1899 by MacDonald, the British representative at Peking. The Chinese silence was taken as acceptance. The British accepted boundary with Russia at Karakoram Pass in 1873 and China erected a boundary pole at the Pass in 1892.

Thus, in the early twentieth century Tibet became the buffer between China, Britain and Russia. British troops entered Tibet in the guise of a trade mission and concluded of a bilateral Treaty in 1904 between Tibet and Britain, on unequal terms,but signifying the independent status of Tibet. China never accepted the treaty. In 1906 China concluded a treaty with Britain that prevented Tibet from concluding direct negotiations with any foreign power without the Chinese consent.

Tibet was brought under direct Chinese rule through a military campaign (1907 to 1911) but Manchu dynasty got overthrown by Sun Yat Sen revolution in 1911 and Tibet reverted to its former status as an independent country.A TREATY OF FRIENDSHIP AND ALLIANCE signed by Tibet with Mongolia, given below,confirms Tibetan independence;

Concluded Between the Governments of Mongolia and Tibet at Urga; 29 December 1912 (11 January 1913).

Mongolia and Thibet, having freed themselves from the dynasty of the Manchus and separated from China, have formed their own independent States, …….

Article 1. The ruler of Thibet, Dalai Lama, approves and recognizes the formation of an independent Mongol State……

Article 2. The ruler of the Mongol people, ChjebzunDamba Lama, approves and recognises the formation of an independent (Thibetan) State and the proclamation of the Dalai Lama as ruler of Thibet…….

After the Soviet revolution, when Russians advanced into Xinjiang, the British in 1927, adopted Johnson -Ardagh line, as a boundary from Afghanistan to Karakoram Pass, to include Aksai Chin and Karakash river in Indian territory.

Indian Claims:

Thus, based on imperial British cartography of shifting boundaries in the Western Sector, India inherited and persisted with the whole of Aksai Chin as a part of erstwhile Kashmir state integrated into India.

By November 1947, India had the following historic treaties defining her territorial boundaries with Tibet:

- The McMahon Line to the east, extending for 890 kilometers from Bhutan in the west to 260 km east of the great bend of the Brahmaputra River in the east, largely along the crest of the Himalayas.
- The map of the erstwhile princely State of J&K(as defined by the Johnson-Ardagh Line of 1897): India had inherited Aksai Chin as part of J&K state without any communication, administration or settled population in Aksai Chin.
- The Treaty of Chushul of 1842: the J&K Maharaja was referred to as the ruler of J&K and Tibet, of the areas of eastern Ladakh, including Aksai Chin as well as the territory he controlled inside Tibet such as Minser estate, comprising a cluster of villages located 296 km deep inside Tibet at the foot of the holy Mount Kailash on the bank of Manasarovar.

So, Indian engagement with and claims on Tibet were considerable. The British had successfully created and maintained a friendly buffer between the contesting powers.

In 1950 Tibet was annexed by the People's Republic of China.There was little Indian protest at the annexation of Tibet by China. The first Indian PM, Nehru's policy of gratifying the Chinese was not reciprocated. Sardar Patel wrote a prophetic letter to Nehru on 7 November, 1950, predicting that China was a potential enemy.His letter (drafted by GS Bajpai, then FS) warned of dire implications for India but it was ignored.

We gave away the Tibetan buffer by signing Panchasheel (five principles) in the preamble of the "Agreement on Trade and Intercourse between the Tibet region of China and India" on April 29, 1954 in Beijing. Apparently, the agreement was about trading and pilgrimage rights but on May 15, 1954 Nehru admitted to the Parliament that the agreement had sealed the fate of Tibet, a peaceful independent nation, which was suddenly deprived of its autonomy.

"So far as Tibet is concerned, it is a recognition of the existing situation there," Nehru stated. For him, the most important feature of the Agreement was not the fate of the Tibetans, but the 'wider implications for world peace'.

For that, India sacrificed a peaceful border with Tibet and gave away the buffer created and cultivated by the British, since the eighteenth century.

This acceptance of Chinese claims over Tibet without settling Sino-Indian border, was a Himalayan blunder.India gave up her consulates and garrisons in Tibet, accepted Tibet as part of China, supported Chinese stand on Taiwan, lobbied for PRC to become Permanent Member of the UNSC and side-lined the Dalai Lama, without any quid pro quo.

Tibetan rebellion was crushed in 1959.In 1962, the PLA attacked and advanced up to the 1899 MacDonald Line which is generally now the Chinese claim line as was also articulated in 1959.In 1962, the People's Liberation Army advanced up to the 1899 MacDonald Line and is generally now the Chinese claim line, articulated in 1959.[3]

Ukraine

In the European continent, historically, the Polish buffer was created and destroyed by the prevalent continental powers, at will. Poland as a state survived, prospered or vanished as per the convenience of continental powers, be it France, Germany or Russia. Ukraine's fate was no different.

The word Ukraine literally translates as 'borderland'(between Poland and Russia). East Ukraine is mostly inhabited by descendants of Orthodox Russians while West is dominated by Catholics with west European influence. Since the establishment of Kievan Rus (882AD) there has been a love-hate relationship between Russians and Ukrainians who spoke nearly the same language till the thirteenth century. Ukraine has been part of Poland, Lithuania, Russian and Austro-Hungarian empires at various times in history.

Ukrainian nationalists:

The Ukrainian War of Independence (1917-21) produced an independent state but the Bolshevikssseized control (1922) creating the Ukrainian Soviet Socialist Republic in the Soviet Union. Ukrainian nationalists like Stepan Bandera, Andrei Melnik and Mikola Lebed never accepted the union and sided with Nazi Germans in the WW-II. They have been accused of leading pogroms of Poles, Jews and Russians as well as political assassinations. During the Cold War Ukrainian nationalists were cultivated by MI 6 and CIA. The nationalists have now morphed into the 'Azov Battalion' (upgraded into

a full regiment in 2015; has foreign soldiers)or 'Kraken' units that proudly display Nazi symbols and was banned by the USA as a terrorist organisation. After Euromaidan revolution, the same fighters were taken into Ukrainian National Guard, armed and trained by the USA to fight the Russians. (Most of these fighters were either killed or captured by the Russians after the fall of Mariupol, in the recent conflict.)

Nuclear renunciation:

At the time of independence Ukraine (1991), had 176 intercontinental ballistic missiles (ICBMs), including 130 liquid fuel SS-19 and46 solid fuel SS-24, as well as 44 strategic bombers armed withcruise missiles, close to 2000 strategic nuclear warheads and 2600 tactical nuclear weapons.[4]

In order to persuade Kiev to abandon the nukes, US President Bush, promised assistance to develop Ukrainian conventional forces (1992 letter). Ukraine did not have technical capacity or finances to maintain this huge nuclear arsenal. Hence, Kiev agreed to nuclear disarmament on the basis of Budapest Memorandum (Dec 5, 1994). According to the memorandum, Russia, the US and the UK agreed to the following:

1. Respect Ukrainian independence and sovereignty in the existing borders.
2. Refrain from the threat or the use of force against Ukraine.
3. Refrain from economic coercion designed to subordinate to their own interest the exercise by Ukraine of the rights inherent in its sovereignty and thus to secure advantages of any kind.
4. Seek immediate Security Council action to provide assistance to Ukraine if they "should become a victim of an act of aggression or an object of a threat of aggression in which nuclear weapons are used".
5. Refrain from the use of nuclear arms against Ukraine.
6. Consult with one another if questions arise regarding those commitments.[5]

NATO Expansion:

The end of WW II saw the beginning of the Cold War between the West-USA and the Soviet bloc. The Soviet Union used Warsaw Pact nations (all had Russian military contingents stationed on their soil)as buffers against NATO in Europe that disappeared after the termination of the Warsaw Pact in

February 1991 and the dissolution of the USSR in December, 1991.Historian Mark Kramer mentions US Secretary of State, James Baker's 1990 talks with Soviet leader Gorbachev.Baker had suggested that the German reunification negotiations could result in an agreement where "there would be no extension of NATO's jurisdiction for forces of NATO one inch to the east," inter alia, applying it to all of Eastern Europe.[6]

In spite of unwritten assurances on NATO expansion,Czech Republic, Hungary and Poland joined NATO on 12 March 1999; Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia joined on 29 March 2004; Albania, Croatia on 1 April 2009; Montenegro on 5 June 2017 and North Macedonia on 27 March 2020. Thus 14 East European states had joined NATO by 2020.

Meanwhile, in 1997 Russia and Belarus had signed a Treaty of Union but NATO was creeping closer to Russian borders.

In February 2007, Mr Putin rejected western assurances that NATO's expansion was not directed against Moscow. "I think it is obvious that NATO expansion does not have any relation with the modernisation of the alliance itself or with ensuring security in Europe. On the contrary, it represents a serious provocation that reduces the level of mutual trust. And we have the right to ask: against whom is this expansion intended?"

However, it was Bucharest summit of NATO (April, 2008) that alarmed Russia. Para 23 of the NATO Declaration stated:

'NATO welcomes Ukraine's and Georgia's Euro-Atlantic aspirations for membership in NATO. We agreed today that these countries will become members of NATO. …….. MAP (Membership Action Plan) is the next step for Ukraine and Georgia on their direct way to membership. Today we make clear that we support these countries' applications for MAP. Therefore, we will now begin a period of intensive engagement with both at a high political level to address the questions still outstanding pertaining to their MAP applications.'

The Russian president, Vladimir Putin, immediately warned that Russia would view any attempt to expand NATO to its borders as a "direct threat". (Georgia in Transcaucasia, was Russian buffer with the Middle East while Ukraine was Moscow's buffer with the NATO). He then, warned that Russia could target rockets at Ukraine if it joined NATO and housed its military bases.

Germany insisted that it was not the right time and their Chancellor, Angela Merkel thought that from Putin's perspective, admitting Ukraine would be a

declaration of war. It was a "red line" the NATO should not cross. Ukraine is seen as the cradle of the Russian nation. Besides, there could be implications for Russian Black Sea fleet based at Sevastopol in Crimea, Ukraine. For Kremlineven Georgian membership was potentially destabilising, due to disputed status of Georgia's separatist regions of Abkhazia and South Ossetia, both having close ties with Russia.

The US was strongly in favour of admitting Georgia and Ukraine to the MAP but Germany, France,Italy, Belgium and Spain opposed stating it would agitate Russia. Ultimately, NATO deferred action on MAP for both Georgia and Ukraine.

War in Georgia - the first Russian counter-measure to NATO Bucharest Declaration:

Transcaucasia is a "buffer zone" between Russia and the Middle East, that borders Turkey and Iran. Besides its strategic importance,Transcaucasia has major petroleum reserves.On 15 July, 2008 US began a joint US-Georgian exercise 'Immediate Response 2008', including servicemen from Ukraine, Azerbaijan and Armenia. After that, anticipating further trouble from Saakashvili government in Georgia, Moscow used separatists and Russian troops to occupy Abkhazia (on Black Sea coast) and South Ossetia enclaves of Georgia. Russia recognized them as independent republics (26 August, 2008).Thus, Putin had made it clear that 'direct threat' to Russian security would be responded immediately.

This was the first Russian counter-measure to Bucharest Declaration which had crossed Russian red lines. The second would follow six years later.

UK and USA in Ukraine

In spite of deferment of NATO membership, UK and USA kept working on Ukraine and seeking regime change to turn it into an anti-Russian bulwark.

UK had historic interest in Ukraine, especially in Crimea and Black Sea. UK and France had fought the Crimean War (1853-56) to shore up the Ottoman Empire and prevent Russian expansionism in the Near East.Then, after the Bolshevik revolution in Russia (1917), UK as a part of the Allied Powers had worked to overthrow the Bolsheviks. According to William Henry Chamberlin, "Downing Street contemplated a protectorate over the Caucasus and the Quai d'Orsay over Crimea, Bessarabia (now Romania) and Ukraine" and began funding White Russian (opposed to Red Bolsheviks) generals.[7]

Since the end of the WWII, UK and USA intelligence services were in touch with Ukrainian nationalists. After the Bucharest setback, USA followed the developments in Ukraine closely. Ukrainian president Yanukovych was elected in 2010 in balloting that international observers considered reasonably free and fair. Corruption and declining economy raised public anger. When Yanukovych rejected the European Union's terms for an association agreement (2013) which had a 'military security' (read NATO) related clause as well, in favour of a Russian soft loan offer, demonstrators occupied Kiev's Independence Square, known as the Maidan, as well as venues in other cities.

Sen. John McCain (R-AZ), of US Senate Armed Services Committee, went to Kiev to show solidarity with the Euromaidan activists. He appeared on stage in Maidan Square during a mass rally.Victoria Nuland, US Assistant Secretary of State for European and Eurasian Affairs travelled to Ukraine three times after the start of the demonstrations. She attended the Maidan on December 5, 2013 distributing cookies to anti-Yanukovychdemonstrators. Her telephone call with US Ambassador to Ukraine, was intercepted by the Russians and leaked to the press,discussing candidates in a post-Yanukovych government.130 individuals died during these'democratic protests' including 18 police officers lynched by the protesters. On Feb. 22 there was a coup and

Yanukovych fled to Russia. On Feb 23, Ukrainian Parliament repealed Minority Language (Russian) Laws and Ukraine got an anti- Russian government.[8]

On Feb 27, the Russians moved.

Crimean occupation – the second Russian counter-measure to NATO Bucharest Summit:

In February 2014, Russian forces occupied Crimea. Separatists backed by Russia 'liberated' large areas of Donetsk and Lugansk border regions from Kiev's control.After 16 March referendum, on 17 March, Crimea declared independence and on 21 March it joined the Russian Federation. Ukraine protested this violation of Article 1 of the Budapest Memorandum.

Putin had earlier retorted, describing the Euromaidan as a revolution. He added,"…. a new state arises, but with this state and in respect to this state, we have not signed any obligatory documents".[9] His deputy, Medvedev stated that Russia had no obligation to "force any part of Ukraine's civilian population to stay in Ukraine against its will". In fact, Russia accused US of violating the Budapest Memorandum by instigating Euromaidan coup.[10]

US/NATO training Ukraine's Forces:

Since the Crimean annexation in 2014, the US and partner militaries have trained and built Ukraine's forces from nearly 100,000 troops to nearly 250,000. US military's contingent of about 300 soldiers have been training them using Joint Multinational Training Group-Ukraine, at Yavoriv Combat Training Centre in western Ukraine. They built Kiev's military training infrastructure and helped the Ukrainian military become NATO-interoperable. Other NATO members included Poland, Estonia, Lithuania, Canada, and UK. Thousands of western intelligence operatives, special forces, and mercenary contractors (US/UK and French) were later embedded with front-line Ukrainian forces. (Several have since been killed or captured.Many operatives coordinated the reception, interpretation, and "actionable" use of highly prized and even more highly classified US/NATO "ISR" (Intelligence, Surveillance & Reconnaissance data.)

Apparently, Ukrainians were being trained in anti-terrorism operations. US had supplied non-lethal military help like, Humvees, medical supplies, bulletproof vests and radars to track artillery shells, Javelin anti-tank and anti-radiation missiles, etc.to fight terrorists (Russian-backed Separatists). US treated eastern Ukraine's Donbass as an Anti-Terrorism Operation zone, or ATO.[11]

The Minsk Agreements

To end fighting between Ukraine and separatist forces in the Donbass region,the first Minsk Protocol, was drafted by the Trilateral Contact Group comprising Ukraine, Russia, and the Organization for Security and Co-operation in Europe (OSCE), helped by France and Germany. The agreement was signed (5 September, 2014) by representatives of the Trilateral Contact Group and, without recognition of their status, by the representatives of Donetsk People's Republic (DPR) and Lugansk People's Republic (LPR).

The agreement, endorsed by UNSC, failed to stop fighting and a revised and updated agreement, Minsk II (12 February, 2015) that had various measures, including a ceasefire, withdrawal of heavy weapons, release of PoWs, granting self-government to Donbass and restoring control of the state border to Kiev. The fighting never ended and the agreement's provisions were ignored.

Ukraine–UK Naval Agreement

On 21 June 2021, UK and Ukraine signed a naval cooperation agreement at Odessa, whereby UK would sell two refurbished Sandown-class minehunters,construct eight small missile warships, a new naval base on the Black Sea for Ukrainian Navy and a base on the Sea of Azov. The agreement included the sale of missiles to Ukraine and for training and support for these.[12]

On 23 June 2021, HMS Defender undertook a 'freedom of navigation' patrol through the disputed waters of Crimean Peninsula. Russian coast guard fired warning shots and a Sukhoi Su-24 dropped bombs in the path of Defender. Russia warned that in future,it would bomb not only the path, but also the target. Putin accused UK of "deliberate provocation" and added that US had sent a plane to monitor the Russian response.[13]

Three Swords 2021

This military exercise involving the Lithuanian-Polish-Ukrainian Brigade, was conducted (July 23-27, 2021) at the International Peacekeeping and Security Centre in Yavoriv, Ukraine, near the Polish border to assess the level of skills of the Lithuanian-Polish-Ukrainian Brigade during a conditional defence mission.More than 1,200 Lithuanian, Polish, Ukrainian and US servicemen,with over 200 combat vehicles participated.[14]

On Dec 1, 2021, Russian foreign ministry accused Ukraine of deploying half of its army or 125,000 troops to Donbass.[15]

The Special Military Operation

UK/US involvement in Ukraine was relentless and alarming. Sensing attack on Donbass region, Russia officially recognised the Lugansk and Donetsk people's republics (21 February 2022)and declared that the Minsk agreements "no longer existed", as Ukrainian Parliament, Rada, had failed to bring reforms and implement their provisions.

"The special military operation of the Russian Armed Forces, carried out since February 24, anticipated and foiled a large-scale offensive by Ukrainian troop strike groups in the Lugansk and Donetsk People's Republics, which are not controlled by Kiev, in March this year," declared Russian Defence Ministry. It claimed that Russian military personnel possessed secret documents of the Ukrainian National Guard directives for an offensive operation in Donbass in

March 2022.[16]

The primary aims of the special military operation announced by Putin were to protect Russian speaking population of Donbass, demilitarise and de-nazify Ukraine. Change of regime was not a priority as that does not achieve demilitarisation. The Russian military armoured column, stretching over scores of kilometres in March 2022, was to demonstrate that Kiev's airpower had been neutralised and force Ukrainians to divert their forces from Donbass region. This was a classic 'feint and fix operation'.Since then, Russia has been systematically destroying military targets and Ukrainian army, especially eastern Ukraine.

Nazis, in the form of Azov brigade have been killed or captured at Mariupol.Besides the notorious neo-Nazi "Azov Battalion", who were armed and trained by US/NATO,the forces in Mariupol also included many dozens of NATO "advisors" (CIA, special forces, and so-called "contractors"). Also present were ~2500 foreign mercenaries, most of them NATO veterans of the wars in Iraq and Afghanistan.

Meanwhile, the West/US have imposed extensive economic sanctions on Russia, recommended in the Rand Corporation report, 'Overextending and Unbalancing Russia; Assessing the Impact of Cost-Imposing Options'. 2019 Rand paper warned US of failure using Ukraine to provoke Russia.[17]

Russians may temporarily halt' special operations' when they have acquired enough territory to keep DPR and LPR out of Ukrainian artillery range. If that does not lead Ukraine to negotiations, Russian ambitions may increase further.

The Buffer

However, all these aims are subsumed by the main Russian goal, viz., keeping the Ukrainian buffer, neutral, if possible or neutered, if not, between Russia and NATO. As mentioned by George Friedman,

'For Russia, the problem is that the Ukrainian border is less than 300 miles from Moscow, and Russia has survived multiple invasions only by virtue of Moscow's distance from invaders – a distance that the collapse of the Soviet Union closed. Russia's obsession with Ukraine is intended to rectify that problem. …….

Russia is attempting to reclaim strategic depth, and it went into it knowing full well the financial consequences it would create. In other words, it put up

with financial damage in exchange for strategic security. So far, it has not gained strategic security and has absorbed significant financial damage while meting out some of its own to Europe.' [18]

So, the special operation may take a breather when the Russians occupy territories east of Dnieper, including Odessa and a secure land bridge to Crimea, possibly up to Transdniestria (unrecognised independent republic) on the Moldavian border, where the Russians have stationed (peacekeeping) troops since 1992. That would leave a demilitarised rump of Ukrainian state as the buffer between Russia and NATO.

Thus ends the comparative tale of two buffers, Tibet and Ukraine.As a historical great power, Russia knows the utility and the necessity of having buffers between its territory and the competing powers. Independent India could have been much more secure had we retained the Tibetan buffer or traded it for a secure India-China border. Realpolitik always trumps idealism.

END NOTES

1) *Ziring,1986:153*

2) *'Lorne J. Kavic, India's Quest for Security: Defence Policies, 1947–1965 (Berkeley: University of California Press, 1967) p. 9.*

3) *(http://www.indiandefencereview.com/news/tibet-the-real-issue/; 'Dealing With the Dragon- Harsh Reality, Hard Options' by Lt General NS Brar (Retd); 'Ladakh after Article 370', by Ambassador P. Stobdan; IE dated 6 Aug 2022)*

4) *William Potter, The Politics of NuclearRenunciation: The Cases of Belarus, Kazakhstan, and Ukraine,Occasional Paper; Washington, DC: Henry L. Stimson Centre, April1995.*

5) *(Philipp Bleek, 29 April 2014; "Why Ukraine wasn't a nuclear power in the early 1990s and the West has no legal obligation to come to its aid now". Arms Control Wonk.)*

6) *Kramer, "Correspondence: NATO Enlargement—Was There a Promise?"; 'International Security', 1 July 2017).*

7) *John W. Long, "Plot and counter-plot in revolutionary Russia: Chronicling the Bruce Lockhart conspiracy, 1918." Intelligence and National Security 10#1 (1995): 122–143.)*

8) *(America's Ukraine Hypocrisy; AUGUST 6, 2017 • COMMENTARY By Ted Galen Carpenter, Senior Fellow, CATO Institute)*

9) *Putin at a press conference, 4 March 2014 (in Russian)". YouTube. 4 March 2014.)*

10) *(Medvedev: Russia does not guarantee the integrity of Ukraine; bbc.com. 20 May 2014.)*

11) *('In Ukraine, the US Trains an Army in the West to Fight in the East', by BEN WATSON,Sr. Multimedia Editor, Oct. 5, 2017; https://www.defenseone.com)*

12) *("UK signs agreement to support enhancement of Ukrainian naval capabilities". GOV.UK. Ministry of Defence. 23 June 2021.)*

13) *(Bennetts, Marc on 30 June 2021; "Putin accuses Britain of provocation over HMS Defender", The Times.)*

14) *('Multinational military exercise 'Three Swords 2021' in active phase'; JULY 27, 2021https://www.thefirstnews.com)*

15) *(MOSCOW, Dec 1, 2021; Reuters).*

16) *(https://www.telesurenglish.net March 10, 2022)*

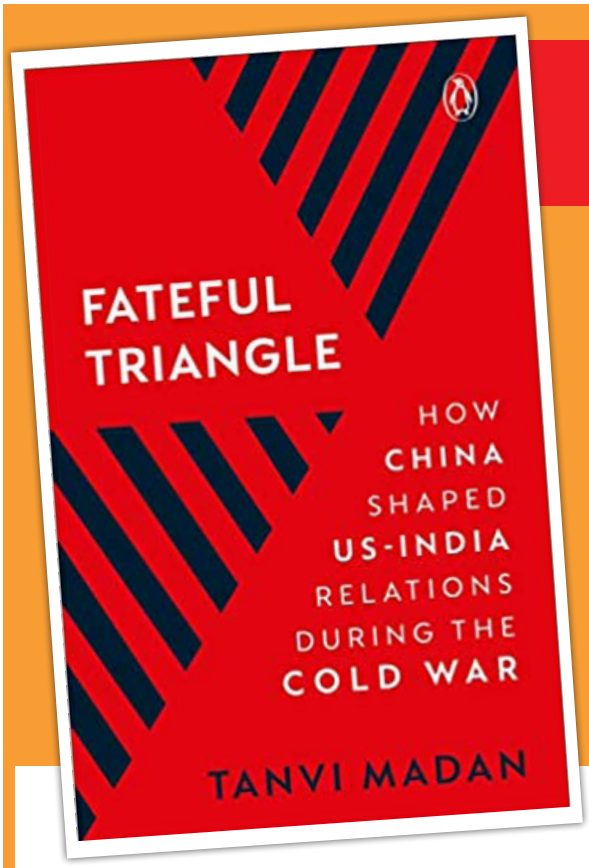
17) *(https://www.rand.org/pubs/research_briefs/RB10014.html)*

18) *GPF; China and Russia's Strategic Problem by George Friedman - August 15, 2022*

ABOUT THE AUTHOR

SHRI JAYANT UMRANIKAR

Shri Jayant Umranikar retired on Dec 31, 2009 after nearly 37 years of outstanding service to the society in various capacities. Since retirement, he writes guest columns on security related and strategic issues in news papers/journals and participates in TV debates on the topical issues. He also works as a consultant on 'vigilance and security related issues for private sector companies. He is the honorary chairman of the International Longevity Centre – India (ILC-I) that looks after the problems of the elderly citizens and Community Aid Sponsorship Programme (CASP) that takes care of underprivileged children.



Book Review

FATEFUL TRIANGLE

How China Shaped US-India Relations During the Cold War

Author : Tanvi Madan

Publisher : Penguin Random House India 2020

BY GP CAPT PRAVEER PUROHIT

The geo-politics of the cold war was a difficult period for India, wherein it had to maintain its 'non-alignment' and yet be mindful of its security and developmental challenges. India's independence and evolution as a democratic republic built on the foundation of equality and pluralism enabled it to have many commonalities with USA. At the same time, India tried its best to have a stable and friendly relationship with China. Following the overthrow of the Nationalists led by Chiang Kai Shek by the Mao led communists, mistrust and ideological differences arose between US and China. Very soon, the Chinese annexation of Tibet resulted in India and China sharing a border that was neither demarcated nor delineated. Beneath the veneer of building bridges of friendship, there lurked mistrust and apprehension in both US and India, about China. It was under such compelling circumstances that Chinese actions influenced US-India relationship in the aftermath of independence.

In Fateful Triangle, Tanvi Madan brings out that China's influence on India-US relations is not a recent phenomenon but dates back to 1949. The author draws

upon extensive research to analyze policy challenges and decisions that shaped the way India and USA engaged with each other. In all these engagements that defined the relationship, the most influential factor that stood out was China. The book examines India-US relations from 1949 to 1979 and how perceptions in Delhi and Washington about China in these three decades characterized how these two countries behaved with each other. In what could be an astonishing discovery for many, Tanvi Madan coherently writes about the considerable time and effort invested by both US and India in their relationship against the backdrop of a delinquent China.

The book is divided into four parts with eight chapters. It takes a chronological approach while examining the India-US relationship in many dimensions. It traces the relationship through phases of divergence, convergence, dependence and disengagement. In each part/ chapter, the author analyzes various factors, their interpretations in Delhi and Washington and why the outcomes were what they were. Part I focuses on the period from 1949 to 1956 when Indian and US perceptions of and policies towards China cast a relatively dark shadow on US-India relationship. Part II examines shifting Indian and US attitudes and actions towards China that drove the two countries together. The period from 1963 to 1968 is covered in Part III. The argument in this part is on the common perception of China as a major threat but differences on the right approach. Notwithstanding the differences, the author pertinently points that this period witnessed military aid into India and assistance in capability building by the US. Part IV delves into shifting perceptions and impact of a developing détente. Ms Madan convincingly argues that although India and US had differing world-views, they were fairly convergent on the Chinese challenge and the need to tackle it. Particularly interesting is the threat of communists in subverting the Indian state and efforts to forestall it.

As one reads through the book, the reader cannot help but be wiser on many unknown facts of history. The book corrects many myths that have emerged out of popular narratives especially with regard to Nehru and US economic and military aid to India. It also shatters the propagated falsehood of unreliability of US. Without being partial or judgemental, the author is able to bring to fore the turning points/events in the relationship as also attitudes, ideology, geo-politics, internal politics and interests that shaped these.

As the strategic partnership between India and USA once again gains strength, it is essential for students, strategic thinkers and policy makers to deep dive into history and understand the drivers of this relationship. The book enriches our understanding of the possibilities and limits of US-India cooperation in the face of an expansionist China. Importantly, it is largely successful in lucidly articulating

the economic and military aid provided by US to India despite the role of internal spoilers on both sides. Fateful Triangle offers an insightful treasure of knowledge. The lessons it brings in foreign policy, addressing strategic challenges from China and harnessing the potential of shared values are extremely relevant in these troubled times. Reading through the book, one cannot but wonder whether the potential of the India-US relationship was under-utilized. This raises pertinent questions. Could the unbridled rise of China have been avoided or checked in time? When we look at the India-China problem through the prism of the multi-domain strategic threat that we face from China, were the opportunities of the past missed ones?

The author's effort in providing an antidote to historical amnesia is indeed laudable. 74 pages of end notes and bibliography give an idea into the monumental research undertaken by the author. The result is evident in the quality of the book. However, one needs to frequently go back while reading as it takes some time to assimilate and connect the happenings. Aptly titled, Fateful Triangle provides enough food for thought with regard to the relationship between India, USA and China. It correctly analyzes that the history of this triangle is too important to be ignored, especially since it will be far more fateful than the past. The reader will realize that in this triangle, the India – US relationship will require patience, perseverance and pragmatism. And although nature may bring the two countries together, sustaining the relationship will require careful nurturing. The book enhances the intellectual and knowledge band width of the reader. The content stimulates the mind to apply logic and reason to a complex issue. It is recommended as a 'must read' for the strategic community, policy makers, students of international relations and especially the Armed Forces.

ABOUT THE AUTHOR

GROUP CAPTAIN PRAVEER PUROHIT

Group Captain PraveerPurohit is an alumnus of NDA and graduated from there in 1989. He was commissioned into the flying branch of IAF in 1990. He has over 5500 hours of flying over all types of terrain in the country. He also has flown extensively in Bhutan and Mauritius. A Qualified Flying Instructor, the officer has trained pilots from all three services, ICG and Mauritius Police Force. The officer was the winner of the Lt Gen SL Menezes Essay Competition 2020 conducted by USI. His articles have been published in USI Journal, CAW Journal and Blue Sky.

EMERGING CYBERSECURITY THREATS IN INDIA : A REASSESSMENT OF INDIA'S NATIONAL CYBER SECURITY POLICY

BY NEERAJ SINGH MANHAS[1] AND HARI YADAV G [2]

[1] Director of Research, Indo-Pacific Consortium, Raisina House, New Delhi.

[2] ICSSR Doctoral Fellow, Centre for South Asian Studies,
Pondicherry (Central) University.

Abstract

Cyber security is connected with ensuring safe cyberspace -secured from threats and online crimes including attacks on digital sovereignty. India has recorded massive 36.29 lakh cyber security incidents from 2019 to June 2022. These numbers are concerning as India is becoming the centre of multiple supply chains and technological hubs - employing and producing great minds. Due to its technological development, India is considered the top choice of investors as well as business operators. In the wake of an upsurge of businesses coming to India and having the responsibility of having the highest population, it becomes imperative for the government to have a pre-defined and secured digital world with laws and regulations for the possible crimes and loopholes that can be exploited by new companies. Even though, the Government of India has laws, acts, and policies to address cybercrime. However, there's a need to bring changes in contemporary laws to keep up with the changes in the cyber world. The article aims to highlight the policy infrastructure of India to address cybercrime and recommend changes in the existing laws according to the different incidents in the recent past. This article also highlights the shortcomings in terms of infrastructural requirements for curbing cybercrime.

Keywords: Cybersecurity, Cyberthreats, cyberterrorism, cyberwarfare, Security.

Introduction

India with a total population of 1.40 billion by January 2022, with 653 million active internet users (or 47% of the total population) and the rest of the population who is inactive or does not have access to the Internet (Kemp, 2022). According to Statista research, India ranks second in the world regarding active internet users, behind China. It is expected that India will add 650 million more, active users, by 2023 (Statista, 2022). With the rapid increase in Internet users across the country, everything has changed and changed gradually while the majority of Indians actively use the Internet in their day-to-day life, at the same time they are unaware of the vulnerabilities and risks involved (Singh, 2016). This has become a major concern for nations in combating cybersecurity threats evolving in cyberspace. Cybersecurity threats can be hacks, security breaches, and harmless threats and some have a huge imp on businesses.

The practice of shielding computers, electronic systems, mobile devices, and data from unsanctioned access and information leaks is referred to as "cybersecurity" (Rao, 2018). Cybersecurity is primarily concerned with protecting user data and preventing unauthorized access to digital equipment connected to the Internet or another network. It took scientists several years after the invention of the computer to invent the Internet, which was barely accessible at the time, but the internet is now available to anyone who owns a mobile device or any other electronic gadget. In today's world, the majority of business transactions, regardless of the domain, are operated through the Internet. Although the Internet is well known for its numerous benefits to individuals, the citizens lack adequate knowledge about using the Internet and face threats in cyberspace, by providing access to cyber-terrorists and hackers without their knowledge to control their devices (Rao, 2018). To avoid those threats, the government and the citizens have to create awareness programs about Data security, Application security, Network Security, Mobile Security, End-user education security, etc., which helps in overcoming the challenges of securing and safeguarding the end-to-end encryption of user data (Bhatia, 2022).

Conceptual Meaning of Cybersecurity in the World vis-à-vis India

According to the World Economic Forum, Global Risk Report 2021, Cyberattacks and data fraud were merged into the failure of cybersecurity measures. And cybersecurity failure has been identified as one of humanity's

most severe challenges over the next decade. (WEF, 2021). The term "cybersecurity," according to the International Telecommunication Union, refers to a collection of tools, training, policies, actions, guiding principal, safety thoughts, and risk management approaches. As the goal of cybersecurity is to accomplish and maintain the security characteristics of an organizations and its user's resources against pertinent safety dangers in the cyber environment. (ITU, 2009). In the United States of America, The United States president has signed an exclusive order to construct the Cybersecurity and Infrastructure Act (CISA), which would protect American cyber networks and cyber infrastructures, this design would help US cybersecurity formations, and create capacity to counter cyberattacks (Juyal, 2021).

In 2017, Israel released its first-ever National Cybersecurity Strategy, which outlines the country's strategy for improving cyber robustness, civilian national cyber defence, and systemic resilience (Frei, 2020). According to the Israeli government, implementing the cybersecurity policy will prioritize its economic, business, and social interests in cyberspace (NIST, 2017). In the United Kingdom, the National Cybersecurity Programme was announced in 2015 to shield its computer systems from cyberattacks. In 2016, the United Kingdom in one of its five-year national cyber security strategies aimed to create its cyberspace to be resistant to cyber-attacks by 2021(HM Government, 2016).

In the Indian context, according to the Information Technology Act of 2000 Cybersecurity risks or cybercrimes are frequently referred to as a range of modern offenses that have progressed as a consequence of the misapplication of digital skills. (Naha, 2022). To combat the cybersecurity threats, the Indian Parliament passed an Information Technology Act, 2000 that came into effect on October 2000. This act is well-known as the fundamental law that addresses the grievances on cybercrimes and electronic commerce. The concept of cybersecurity threats has existed in various forms throughout history. Exposing the phone tapping scandals remained significant in Indian history during the 1980s, though it was limited to politicians and other high-ranking officials. In contrast, cybersecurity is now not only for the state but also for its citizens. The threats are making Indian citizens more concerned about their online privacy and data security, along with government surveillance. (Subramanian, 2016). As a result, the Indian government must provide appropriate education and security on online behaviour to reduce risks and increase the secure online environment for its citizens.

India's Position in Countering Cybersecurity threats

According to Global Cybersecurity Index 2020, India is now ranked 10th position, up from 37th rank in previous years. Though the report has considered only a few parameters during the assessment, it includes legal measures, organizational measures, technical measures, capacity development, and cooperation (PTI, 2021). In the past decade and in contemporary times, India is considered the technological hub which produces great minds. With its due importance to technological evolution, the top IT / MNC organizations are considering India as a top destination for their business operations. Though the opportunities are abundant for technology-based companies, it has also got severe challenges in securing a strong base in cyberspace. Especially, from 2015 onwards India is prone to cybersecurity threats in cyberspace and ranks as the world's second most vulnerable country, after China. And during the Covid-19 Pandemic, the entire work pattern got revolutionized and created a path for more active internet users in India at nearly twice the rate at which cybercrimes or cyberattacks are been reported.

Cybercrimes or cyberattacks can be categorized into different forms of threats occurred in cyberspace, they are;

Cybercrime: Computers are their primary target in this illegal activity, or they may simply be used as a convenient tool to commit any sort of cybercrime, which is conducted through computer networks. (Juyal, 2021). Cybercrime has been around for a while, but as more people are using the Internet and spending more time online, along with the sense of isolation, anxiety, and fear brought during the lockdown, the threats like phishing, hacking, and spamming have increased through the Information technology and evolved in unexpected ways (Naha, 2022), by increasing the opportunities for cybercriminals to profit from the situation or cause disruption and causing damage to many people and businesses including towering economic losses (Steinberg, 2020). According to the CSIS, India's National Cyber Security coordinator declared that cybercrimes in India billed at almost $17 billion in 2019 (CSIS, 2022).

Cyberwarfare: Cyberspace is used as the medium to commit terrible acts of war against other nations, known as cyber warfare. Cyberspace has emerged as the fifth dimension of warfare and tool for offenders, after air, land, ocean, and space (Juyal, 2021). The cyber-attacks include website defacing, distributed denial of service, and so on. Most cyberattacks consist of politically motivated attacks against online information and information systems. Including India, a few more countries are developing sophisticated malicious software as their lethal weapons. Any country will have a significant barrier when it comes

to large-scale mapping of Supervisory Control and Data Acquisition (SCADA) devices utilizing specialized technologies (Brook, 2018).

Cyberterrorism : Barry Collin originally used the word "cyberterrorism" in the 1980s. (Conway, 2003). According to the FBI, cyberterrorism is "any planned, politically driven attack against data, computer systems or programswhich outcomes in violence against non-combatant targets by sub-national groups or clandestine agents" (Marsili, 2018). Cyberterrorism is a generic term for the various activities in cyberspace: the activities mostly involve diverseestablishments, clusters, and individuals (Heickero, 2014). Its main motive is to invade the cyber networks which are responsible for the preservation of national security and terminatedata of strategic status, this is also considered the biggest threat to the security of any country (Scherr, 2016).

The use of the internet to perpetrate cyberterrorist activities is on the rise as it has become so simple for terrorists to link, organise terrorist cells, share evidence, plan attacks, and recruit new members. (Gable, 2009). For example, The US Department of State has cited the 26/11 Mumbai Attacks as the deadliest incident that occurred using the technology in the Indian scenario (Reich, 2012). As additional systems become interconnected and reliant on computer networks, new susceptibilities are being created that can be taken advantage of by malicious persons and organizations. In the early 2000s, there were numerous incidents staged by cyber terrorists, in the different forms of computer viruses, such as Nimda, Code Red, Love Bug, and later Melissa. Finding the brains behind these operations might be challenging in the majority of cases. Because of the Internet, one can remain anonymous as long as they have the necessary skills to erase their digital footprints (Heickero, 2014).

The combination of psychological, political, and economic forces has led to an increase in people's dread of cyberterrorism (Weimann, 2004). In the past decade, since anything simple is done through computers the common phrases like cybercrime, info-war, cyberterrorism, virtual warfare, cyberattack, and digital terrorism are used to characterize what some military and political strategists regard as the "new terrorism" (Naha, 2022). And, the trend continues where cyber terrorists have altered their goals. Mostly the traditional terrorist has moved from moderately simple methods of creating anxiety among individuals to more sophisticated, rational, and purposeful behaviour. One of the well-known examples of cyberterrorism is the way the Al-Qaeda organization uses its technology to advance its political and ideological objectives (Heickero, 2014).

In 1988, Osama Bin Laden established the terrorist organization known

as Al-Qaeda. It is a global movement that has supporters in West Asia and reaches from Algeria to the Philippines. The group is allegedly in charge of carrying out several terrorist strikes in various nations. Al-Qaeda's main objective is to create an Islamic caliphate that would rule all Muslim-populated areas from the Arab world to Southeast Asia. The organization is a part of the Jihad or Islamic political violence. Islam distinguishes jihad into two different forms, such as Jihad Ashgar, also known as small jihad, which is governed by several ethical laws and includes certain political and military aspects, and Jihad Akbar, also known as Greater Jihad. Both are intended to safeguard Islam and its holy places. After the emergence of Information technology with numerous benefits with provided anonymity, the terrorists started to launch their attacks via technology rather than more traditional means. Moreover, the internet/cyberspace is utilized to facilitate their communication and disseminate information to their organization, which is preparing to undertake an attack. Hence, Electronic jihad and cyber jihad are two contemporary phrases that can be used to characterize this progression or transition on the Internet domain (Heickero, 2014).

To combat these emerging cybersecurity threats in various forms, the Indian Government has implemented several policies and regulations aimed at containing cyberattacks or cybercrimes by providing a user-friendly cyber secured space for both citizens and the state.

Information Technology Act, 2000

The Information Technology (IT) Act is passed by Union Government on June 9, 2000. In India, this act was enacted to deal with the cybercrimes committed against people, organizations, and Society (Singh 2016). Further to strengthen the policy, the Ministry of Information Technology reiterated the IT Act 2000 and passed a new amendment on 5th February 2009 known as Information Technology Amendment Act 2008 (MLJ, 2009). This policy focused mainly on Data Privacy, Information Security, Making digital signatures neutral, the Inclusion of additional cybercrimes like Child Pornography and Cyberterrorism, and finally recognizing the role of the Indian Computer Emergency Response Team (CERT-In). The National Critical Information Infrastructure Protection Centre (NCIIPC) has been recognized by the Act as the Nodal Agency for the Protection of Critical Information Infrastructure (CII) (VIF, 2022). In addition, the Union Government formed the Cyber Defence Agency to address issues related to cybersecurity and cyberwarfare. (Pandit, 2019).

Indian Computer Emergency Response Team (CERT-In)

Indian Computer Emergency Response Team (CERT-In) acts as the national watch and alert system in providing advisories on the latest cyber threats. The Union Government established CERT-In to maintain India's cybersecurity and combat threats against the nation (Juyal, 2021). It acts as a nodal agency that deals with cybersecurity threats like Phishing and Hacking (Singh, 2016). It helps the state in gathering, examining, and disseminating data on cybersecurity occurrences, then focuses mainly on issuing alerts about cyberattack response activities. In addition, India formed a domain-specific emergency response team to build a more secure online environment in respective sectors like Transmission, Thermal, Hydro, and Distribution (PIB, 2017). The CERT-In strengthens the security-related defence of the Indian Internet Domain.

National Cyber Security Policy, 2013

India's National Cyber Security Policy was published in 2013. The goal of the policy is to protect Indian cyberspace and increase its concrete resilience to cyber threats across all industries (Meity, 2013). The policy works as a first step in improving India's Cyber security infrastructure, and also it helps to protect the personal information of Internet Users' financial and banking information (Singh, 2016). Due to this regulation, a secure computing environment has been made possible, and tremendous trust and confidence in electronic transactions have grown. The policy framework states that a key component of the fight against terrorism and cyberterrorism is technology and threat intelligence (Juyal, 2021). Moreover, the National Investigation Agency (NIA) Act was amended by the Indian Parliament in 2019 to enable the investigation and prosecution of cyberterrorism (PTI, 2019). Despite the existence of the National Cyber Security Policy, it was unable to stop these attacks planned by the Pakistani government who intended to cate fake government and military websites to deliver malware viruses in March 2022, this is an espionage operation on Indian government employees (CSIS, 2022).

The Indian government has progressively introduced various policies and regulations to combat the cybersecurity threats that are emerging in cyberspace. With the increasing pace of active Internet Users through smartphones, India has become the prime target of cybercriminals and cyberattacks (Subramanian, 2016). Despite its escalation of cyberattacks and cybercrimes reported in India, the lack of cybersecurity professionals and adequate knowledge on using

cyberspace among the citizens remains a major hindrance in the Country.

Challenges Faced by India in countering cybersecurity threats

- **Lack of Awareness:** People in India are aware of using smartphones, but they are not sufficiently informed about the dangers posed by online threats. India has a sizable number of worldwide active Internet users, and that figure is expected to grow over time. It is preferable to educate the public about prevention strategies to stop internet users from being victims of cybersecurity dangers.
- **Lack of Non-Governmental organization participation:** After the introduction of any governmental policy, it is time-consuming when it reaches the citizens. For instance, the Information Technology Act, 2000, after the policy's implementation, took several years for the citizens to understand the policy and its importance. If the civic society groups or NGOs participated in raising citizens' understanding of the policy and its laws that would have been beneficial to them and also help them to avoid cybersecurity hazards on the Internet domain.
- **Lack of Holistic Approach:** India is the second most populous country with a 1.40 billion population in the world. The country has got great minds involved in the Information and Communication Technology sector; it can utilize the experts who are working while drafting the policy recommendations.
- **Lack of Private Sector Unit Participation:** India has been remarked as the destination for top IT giants. The involvement of these private sector firms throughout the policy development process, as well as their insightful thoughts and recommendations, will improve the policy process and prevents organizations from cybersecurity threats in the future. It's a win-win situation for both state and the organization.
- **Lack of Cybersecurity Professionals:** India had got a great pool of talent, but the country lacks cybersecurity professionals. Because of this, the state is forced to rely on other countries to address its problems in cyberspace. Whereas, If India educates its people in the necessary fields, it can stop the cybersecurity assaults and other cybercrimes on the Internet to resolve these issues.
- **International Collaboration:** Cyberterrorism or cyberattacks are crimes that are committed globally. An international agreement with all nations

should be made that is legally binding to defend strategic cyberspace. India must take the required actions and make the necessary efforts to internationalize its domestic laws on cybersecurity or cyberterrorism to increase its international collaboration with other nations.

- **Lack of Security Culture:** Cybercrimes have grown significantly in recent years, particularly during the Covid-19 Pandemic. Every person who regularly uses the Internet has experienced some sort of cyberattack, it can be during mobile banking transactions, paying bills, or using smartphones for different purposes. India must strengthen its cooperation in terms of general security issues to stop such operations (Singh, 2016).

Conclusion

Cybersecurity threats have become a critical issue for all countries across the globe. At present, the primary danger to the nation's security comes in the shape of cyber threats like cybercrime, cyber terrorism, cyber warfare, and so on. A large portion of this country's unskilled population is now a target of cybercrimes, even though cybersecurity is a complex and multifaceted subject with no obvious allies or adversaries. The emergence of Cybersecurity threats has become an important policy issue that affects the security of India. Securing the Critical information infrastructure, which is exclusively linked to the defence industry, energy industry, financial industry, and telecommunication industry, has taken a top priority position in terms of national security. Additionally, the increasing interdependence of nations across borders in cyberspace has prompted the development of cybersecurity as a key element of national security strategy in several nations around the world. To achieve a strong cyber security policy, the government has taken the initial steps in formulating a progressive policy. If repeated cybercrime persists and the number of offenders rises online, then the cybersecurity policy which is created will not be appropriate and it will not provide any suitable protection either to the government or to its citizens. Even after the National Cybersecurity policy, of 2013 came into the existence, there is a lack of awareness among the public and a lack of cybersecurity professionals or experts in the country who can educate the citizens about the advantages and disadvantages of cyberspace to the unskilled population. If India overcomes these two existing issues, then the majority of the problem is solved. A Country like India, which has more active Internet Users needs a cyber-secured policy framework that safeguards both the citizens and State.

References

- *Bhatia, Dr. Deepshikha (2022), "A Comprehensive Review on the Cyber Security Methods in Indian Organisation", International Journal of Advance Soft Computer Applications, Vol.14, No.1, March 2022, Accessed from http://www.i-csrs.org/Volumes/ijasca/2022.1.8.pdf on 24th August 2022.*
- *Brook, Chris (2018), "What is SCADA Security?", Daily Guardian Blog, Accessed from https://digitalguardian.com/blog/what-scada-security#:~:text=SCADA%20Security%20is%20broad%20term,nations%20where%20they%20are%20employed on 28th August 2022.*
- *Conway, Maura (2003), "Cyberterrorism: The Story so far", Journal of Information Warfare, Vol. 2, No. 2, Accessed from https://www.jstor.org/stable/26502767on 28th August 2022.*
- *CSIS (2022), "Significant Cyber Incidents Since 2006", Centre for Strategic and International Studies, Accessed from https://csis-website-prod.s3.amazonaws.com/s3fs-public/220805_Significant_Cyber_Events_0.pdf?ruYyPiNzwADjystZd.g9QgMEPY1K28Et on 28th August 2022.*
- *Frei, Jasper (2020), "Israel's National Cybersecurity and Cyberdefense Posture", Center For Security Studies, ETH Zurich, Accessed from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf on 25th August 2022.*
- *Gable, Kelly (2009), "Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent", SSRN Journal, Accessed from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1452803 on 29th August 2022.*
- *Heickero, Roland (2014), "Cyber Terrorism: Electronic Jihad", Strategic Analysis, Taylor and Francis Group, Vol. 38, No. 4, pp 554-565, Accessed from https://doi.org/10.1080/09700161.2014.918435 on 29th August 2022.*
- *HM Government (2016), "National Cyber Security Strategy 2016-2021", Accessed from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf on 25th August 2022.*
- *ITU (2009), "Series-X: Data Networks Open System Communication and Security", Overview of Cybersecurity ITU-T X.1205, Geneva: ITU, Accessed from https://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf on 25th August 2022.*

- *Juyal, Rebant (2021), "Cybersecurity and Threats: Cyberterrorism and the Order Today", Journal of Defence Studies, Vol. 15, Issue. 2, April – June 2021, Accessed from https://www.idsa.in/jds/cybersecurity-and-threats-15-2-2021 on 25th August 2022.*
- *Kemp, Simon (2022), "Digital 2022: India", Datareportal, Accessed from https://datareportal.com/reports/digital-2022-india on 23rd August 2022.*
- *Marsili, Marco (2018), "The War on Cyberterrorism", Democracy and Security, Taylor and Francis Group, Accessed from https://www.tandfonline.com/doi/full/10.1080/17419166.2018.1496826 on 29th August 2022.*
- *Meity (2013), "National Cyber Security Policy – 2013", Ministry of Communication and Information Technology, Government of India, Accessed from https://www.meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf on 30th August 2022.*
- *MLJ (2009), "The Information Technology (Amendment) Act, 2008", The Gazette of India, Ministry of Law and Justice, Accessed from https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf on 29th August 2022.*
- *Naha, Alik (2022), "Emerging Cyber Security Threats: India's Concerns and Options", International Journal of Politics and Security, Vol. 4, No. 1, 2022, pp. 170-200, Accessed from https://doi.org/10.53451/ijps.996755 on 26th August 2022.*
- *NIST (2017), "Success Story: Israel National Cyber Directorate Version 1.0", Accessed from https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-10 on 25th August 2022.*
- *Pandit, Rajat (2019), "Agencies take shape for special operations, space, cyber war", The Times of India, Accessed from https://timesofindia.indiatimes.com/india/india-begins-setting-up-new-tri-service-agencies-to-handle-special-operations-space-and-cyberspace/articleshow/69346012.cms on 29th August 2022.*
- *PIB (2017), "Four Sectoral Computer Emergency Response Teams to mitigate Cyber Security Threats in Power Systems", Press Information Bureau, Ministry of Power, Government of India, Accessed from https://pib.gov.in/newsite/PrintRelease.aspx?relid=159537#:~:text=The%20Minister%20added%20that%20for,to%20coordinate%20with%20power%20utilities on 30th August 2022.*

- *PTI (2019), "Amended NIA Act with powers to probe abroad comes into force", Press Trust of India, The Hindu, Accessed from https://www.thehindu.com/news/national/amended-nia-act-with-powers-to-probe-abroad-comes-into-force/article28798419.ece on 30th August 2022.*
- *PTI (2021), "India ranks among top 10 in ITU's Global Cybersecurity Index 2020", Business Standard, Accessed from https://www.business-standard.com/article/technology/india-ranks-among-top-10-in-itu-s-global-cybersecurity-index-2020-121063000713_1.html on 27th August 2022.*
- *Rao, Sushma, Nair, Sandeep, Joseph, Moly (2018), "Cybersecurity: What Everyone needs to Know", Accessed from https://www.researchgate.net/publication/354907006_Cybersecurity_What_Everyone_needs_to_know_Cybersecurity_What_Everyone_needs_to_know/stats#fullTextFileContent on 24th August 2022.*
- *Reich, Pauline C (2012), "Case Study: India-Terrorism and Terrorist use of the Internet / Technology", In P. Reich and E. Gelbstein (Eds), Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilization (pp. 377-408), Accessed from https://www.igi-global.com/gateway/chapter/72177 on 29th August 2022.*
- *Scherr, Kendall (2016), "UN Report identifies the Internet as a Major Tool of Terrorists and Discusses Counterterrorism Strategies", Homeland Security Digital Library, Accessed from https://www.hsdl.org/c/un-report-identifies-the-internet-as-a-major-tool-of-terrorists-and-discusses-counterterrorism-strategies/ on 28th August 2022.*
- *Singh, Onkar, Gupta, Priya and Kumar, Roushan (2016), "A Review of Indian Approach towards Cybersecurity", International Journal of Current Engineering and Technology, Vol 6, No.2 (2016), Accessed from https://www.researchgate.net/profile/Onkar-Singh-22/publication/329416415_A_Review_of_Indian_Approach_towards_Cybersecurity/links/5fddad6045851553a0ce23c7/A-Review-of-Indian-Approach-towards-Cybersecurity.pdf on 24th August 2022.*
- *Statista (2022), "Number of Internet Users in selected countries in 2022", Accessed from https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries/ on 23rd August 2022.*
- *Steinberg, Scott (2020), "Cyberattacks now cost companies $200,000 on average, putting many out of business", CNBC, Accessed from https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html on 27th August 2022.*

- *Subramanian, Ramesh (2016), "Historical Consciousness of Cybersecurity in India", WISP 2016 Proceedings, Accessed from https://aisel.aisnet.org/wisp2016/7/ on 26th August 2022.*
- *VIF (2022), "Protection of National Critical Information Infrastructure", Vivekananda International Foundation, New Delhi, Accessed from https://www.vifindia.org/sites/default/files/Protection-of-National-Critical-Information-Infrastructure.pdf on 29th August 2022.*
- *Weimann, Gabriel (2004), "Cyberterrorism: How Real is the Threat?", United States Institute of Peace, Washington DC, Special Report 119, Accessed from https://www.usip.org/sites/default/files/sr119.pdf on 29th August 2022.*
- *World Economic Forum (WEF), Global Risks Report, 16th edition (2021), Accessed from The Global Risks Report 2021 | World Economic Forum (weforum.org) on 24th August 2022.*

ABOUT THE AUTHOR

NEERAJ SINGH MANHAS

Neeraj Singh Manhas is a Director of Research in the Indo-Pacific Consortium at Raisina House, New Delhi. Currently, he is also pursuing his Ph.D. in International Relations (Chinese Studies). He has authored four books and has various research interests covering Sino-Indian border issues, China in the Indian Ocean; India-China Foreign Policy; Water security; Defence and Indo-Pacific studies. His writings have appeared in The Daily Guardian, The Hindu Business Line, The Pioneer, Financial Express, China-India Brief (National University of Singapore), ORF and other online platforms.

HARI YADAV G

Hari Yadav G is an ICSSR Doctoral Fellow, Centre for South Asian Studies, Pondicherry University. He has completed his Master of Arts in Political Science and International relations from St. Joseph's College, Bangalore. His research interests include Geopolitics, the Indian Ocean region, Indo-Pacific, Sino-Indian relations, China's geoeconomic initiatives, and cybersecurity issues. He has published various articles and presented papers at national and international conferences.

INFRASTRUCTURE DEVELOPMENT : AN ENGINE FOR DEFENCE PREPAREDNESS

BY COL YOGESH NAIR

Introduction

Infrastructure is vital to any nation. It is a key driver for national progress and a critical enabler for productivity and sustained economic growth . It is a complex and interdependent system, which provides us with the energy, transport, water and other essentials utilities that are the basis of sustenance of the society and well-being of the people. In effect, infrastructure is the lifeline of country's growth and one of the most crucial elements, which determines the comprehensive power of the Nation State . Similarly, military infrastructure is the corner stone for the national security of any country and its defence preparedness. Good infrastructure adds to the 'teeth' of the armed forces and its availability is of paramount importance for planning all type of military operations. It rightly should precede all requirements of Armed forces including weapons and ammunitions; however, the irony is that the defence infrastructure in India has not got the priority it deserves. A lot of noise is heard in several quarters including media with respect to deficiency of weapons, ammunitions and equipment; but very little is said about the infrastructure requirements for the national security of the Country.

Need for Development of Military Infrastructure

The military infrastructural development has remained hebetudinous, resulting in glaring infrastructural deficit along the Northern borders, whereas, the Chinese have developed a well thought-out military backbone infrastructure right upto the borders that deeply impinges upon the security paradigm along the borders . The infrastructure disparity between India and China determines the military postures and necessitates heavy troop deployment for guarding the borders by India. By 2000, approximately 40% of defenceassets along

the forward line were more than 30 years old and lack of adequate funds for its maintenance further deteriorate its condition . Nonetheless, post 2000 the strategic approach towards defence infrastructure has witnessed some positive shift, and things have started to improve. However, considering the lack of focus, miniscule fund allocation and inconsistency in strategic orientation, the infrastructure apathy along the borders continued unabated. With China, ramping up its infrastructure along the northern borders India's defence preparedness in terms of military infrastructure is grossly inadequate, requiring strengthening of strategic policy for holistic improvement of defence architecture.

Analysing the Criticality

The current Defence infrastructure has evolved over many years. However, these have been developed in a disjointed/ piecemeal manner, without any overarching strategy and hence have not contributed meaningfully in its manifestation including reducing the size of the Armed Forces. At places, the infrastructure has remained underutilized, consequently deteriorating considerably adversely impacting the defence preparedness. It needs to be appreciated that in a worst case scenario during outbreak of war, most of the war fighting requirement of weapons, ammunition and equipment can be provisioned on a war footing however, infrastructure cannot be created over night. Although India has been aggressively pushing to enhance its security architecture and ramping up its defence prowess, it falls short of its objectives in the infrastructure domain.

Limited budget allocation for military infrastructure over many years meant that maintenance and lifecycle replacement of physical assets achieved minimum standards resulting in a steady decline in condition, while the requirement of military infrastructure has increased manifold. Lack of long term perspective and inadequate focus on the projects in the last few decades has suffered from cost overruns and delayed completion timelines. As a result, the criticality is that the present infrastructure requirement cannot be sustained to an acceptable level within the current level of funding.

Considering the changing security dynamics and geopolitical situation in India's neighborhood, the defence approach cannot afford to be the same any more. Losing even an inch of territory is just not acceptable and focus on infrastructure to enhance the level of defence preparedness is a must. With China carrying out massive improvements in the infrastructure upto the borders,

appropriate up gradation of infrastructure on the Indian side cannot be delayed any further. Hence there is a need to thoroughly integrate infrastructure in the defence planning processes and evolve a sustainable infrastructure policy to deliver India's National security objectives.

Attributes of Defence Infrastructure and The Big Picture

A nation's economic strength is reflected in its infrastructural assets. Most developed nations have shaped their Armies mostly through construction of military infrastructure and advanced weapon systems. Defence infrastructure acts as a force multiplier during war as it shortens the critical force readiness time, posturing of strategic resources and facilitates sustained logistic support to the Armed forces. The attributes of well developed defence infrastructure have been deliberated in the succeeding paragraphs.

Development of Full Military Potential

Application of sizable forces at the point of decision in an acceptable timeframe with speed and momentum in the area of own choosing or that is threatened by the adversary is the most important battle winning factor of warfare. Faster induction of troops and material along with a robust frontline including far and inaccessible areas is essential for responsive defence architecture. Hence, a well developed communications network, infrastructure for logistics build-up and well equipped field fortifications will enable application of acclimatized troops for a decisive outcome. It will enable concentration of military forces to maintain a defensive balance, develop operations along multiple axes and enable quick switching of forces. It would facilitate synergised employment of an integrated force to achieve superiority of force level in different stages of battle, thus enabling development of full military potential .

Reduction in Size of Armed Forces

The paucity of defence infrastructure along the Northern borders is one of the major constraints on its ability to effectively wield military power against China. This has led to India's manpower-intensive approach and positioning of large quantum of equipment and supplies in proximity to border for rapid deployment of forces in the event of crisis. Improved border infrastructure will enable India

to station bulk of its conventional forces in the interior to be moved forward only in the event of conflict. A well developed infrastructure would thus obviate the need to maintain a large standing army for the country's defence system resulting in saving of large expenditure, besides improving the effectiveness and efficiency of force generation and employment over a period of time.

Reduced Geographical Isolation

India's North-Eastern region is adversely affected due to paucity of infrastructure, resulting in backwardness and geographical isolation from rest of the country. Underdeveloped North-Eastern states have resulted in people's alienation, anti-establishment sentiments and militancy, affecting the security of the country. Although India, in order to remove the isolation of its North-Eastern region has enunciated its 'Act East' policy with a view to improving its economy and establishing strategic relations with Southeast Asian nations, it has not been able to exploit it fully due to the deficiency of infrastructure . The accessibility to neighbouring countries through a quality road and rail network would pay rich dividends for economic development of northeast India. Hence, development of infrastructure is essential to remove the geographical isolation of these areas and enhance India's status as a reckonable regional power of Asia. Improved border infrastructure could also serve for enhanced cooperation in the field of trade and commerce , while addressing the asymmetry and imbalance between India and China.

Efficient Border Management

With globalization and interdependent world in an international system, the porosity of borders is a challenge to the security forces, requiring an efficient management at the borders . This can be accomplished with construction of smart border infrastructure capable of effective communication and coordination among all security agencies to check organized crime, illegal migration to arrive at a common operating philosophy to neutralize the likely security threats to the country. Improved infrastructure is also essential as part of efficient border management and resolving disputes between the two countries, as the LAC between the two countries is not delineated and based on perception. Having infrastructure in border areas is an opportunity for neighbouring countries to explore more interactions with connected borders and to establish long lasting peace in the region .

Utilisation of Armed Forces Out of Area Contingencies

21st century is an era of dynamic and challenging security environment. India's Regional power status necessitates the Indian military to project itself as a net security provider capable of conducting operations beyond borders including overseas humanitarian and disaster relief operations and evacuation of Indian Diaspora from conflict zones. Thus it needs to conduct activities such as military diplomacy, military support &assistance, capacity building of foreign armies and direct deployment of military forces including United Nation peace missions whenever called for. All this could be made possible when majority of Indian Armed forces are relieved of their conventional role of securing the borders by developing a holistic & robust defence infrastructure.

The Way Ahead

Infrastructure is a 'paramount and essential element' of all national security considerations. Delivery of combat power is dependent upon the availability of infrastructure. Hence the need for building a vibrant defence infrastructure architecture for enhancement of the comprehensive National Power of the Country cannot be overstated. However, there are several challenges to India's road to development of military infrastructure which includes a defensive mindset, shortage of funds, policy shortcomings, technology deficit ,difficult terrain & weather conditions along the Northern borders etc. The way forward for establishment of a strong defence infrastructure would need a complete overhaul of the existing system. Some of the measures towards achievement of the same have been deliberated in the succeeding paragraphs.

Establishment of National InfrastructureCommission (NIC)

The Indian Armed forces hold one of the largest estates in the country which includes both the land and the physical infrastructure. Presently, Ministry of Defence(MoD) is primarily responsible for visualizing and developing the military capability of the Country. This is a huge task and hence planning of defence infrastructure cannot be left to the overworked MoD for a meaningful & holistic policy formulation and focused approach on infrastructure development. Besides, defence infrastructure needs to be considered as functional nation assets ,for larger utilization of nation and its people, necessitating it to be dovetailed in the national infrastructure plan by the Niti Ayog. Hence, there

is a need for establishment of NIC to look after the requirement of military and strategic infrastructure and to integrate these with national infrastructure development plan. NIC of UK &Australia and National Infrastructure Advisory Council (NIAC) of USA have played a pivotal role in effective management of their national infrastructure including military assets.

Revamping Military Infrastructure Organisation

Planning of defence infrastructure is a serious job. In India, presently this is done by number of different agencies viz., Land Warfare & Environment (LWE) Directorate and Military Engineering Services (MES) responsible for Annual Works Programme, Military Operation (MO) Directorate planning requirement of Operational Works, Border Roads Organization (BRO) entrusted with development of border communication infrastructure with Defence Estate Organisation (DEO)handling real estate of the Defence forces. Individuals delegated for defence planning are not experts in the field, deputed for a short duration of timeframe with no specific mandate and knowledge of financial outlay. This results in compartmentalized and piecemeal planning process leading to wastage of valuable resources and efforts. Hence there is a need to establish a Military Infrastructure Organization to manage the estate centrally, cut costs, drive rationalization, create commercial opportunities and undertake long term planning and development of defence infrastructure.

Provisions of Non-Lapsable Defence Infrastructure Budget

The budget for defence infrastructure is always under severe resource crunch. Allocations of funds aregrossly inadequate for meaningful implementation of projects. A major drawback of defence infrastructure is that these are not supported by financial outlay and mostly planned as annual budgets. In Financial Year (FY) 2004-05, a proposal was mooted to formulate Defence budget as a non-lapsable budget, however the plan was dropped citing non-availability of the budgetary rules to carry forward unspent funds. Fortunately, the same has been agreed in-principle by Government of India recently, based on the recommendation of 15th Financial Commission . This is utmost important considering the long gestation period of infrastructure projects and hence modalities & structures need to be formulated on priority to carry forward budgetary allocation of defence infrastructure rather than compulsory booking/surrender of allotted funds in the same FY. Besides, action needs to be taken to revive the Defence Modernization Fund, as also

funding defence infrastructure project through other means.

Integration of Defence Infrastructure with National Infrastructure Plan

Infrastructure requirement is essential for all sectors of Country's development and human well-being. Inclusive progression requires formulation of National Infrastructure plan and implementation of the same requires greater understanding of each sector, their interdependence and need for arriving at a balanced development approach. Hence the traditional silos of government and the resources of Ministries such as Defence, Railways, Road Transport and Highway, Urban Development, Home, Water Resources etc., needs to be effectively integrated. A Strategic Infrastructure Development Body (SIDB) under Niti Ayog needs to be created to play a vital role in supporting the needs of armed forces for planning, integrating and furthering the infrastructure needed for national security. The vision of SIDB needs to provide the defence forces with efficient infrastructure for enhancing the security needs of the country. It needs to prepare strategies for development of defence infrastructure plan for a period of 15 to 20 years, fully integrated with the National infrastructure plan that is optimal and sustainable to meet its strategic requirements at an acceptable level of risk to its military capability .

Public-Private Partnership (PPP)

Considering the huge requirement of funds for defence infrastructure development, the strategy should be to promote private investment where feasible or through some form of PPP. Inhospitable terrain and non availability of labour for carrying out hazardous tasks, requirement of large investment, low profitability, security restrictions and lack of appropriate expertise and equipment have discouraged private enterprises from undertaking defence infrastructure projects in the remote and difficult border areas. Hence policies to attract private investment in a transparent manner with clearly defined responsibilities and an openly competitive bidding process needs to be formulated. India's private sector also needs to change some of its practices, as aggressive bidding and inadequate liquidity drive construction firms to excessively rely on loan financing and shortcuts . Consortiums by reputed builders to pool in resources with capabilities to recycle capital faster for generation of infrastructure funds needs to be explored. Ministry of Finance also needs to examine the area of convergence for financing of PPP projects.

Equal Value Infrastructure

The Armed forces have large amount of land in prime areas that can be bartered with the State Government and autonomous government institutions to generate funds/ equal value infrastructure. There is a need for the Government to recognize the excessive demand of funds that significantly exceeds the annual budget allocation and hence should be prepared to take bold steps to re-locate the defence establishment to lesser attractive locations. Out of the box solution for generating funds to make good the deficiencies of defence infrastructure needs to be explored and planned wherever feasible.

Incorporation of Technologies for Development of Smart Infrastructure

There is a need to adopt use of latest technologies to overcome problems of deficiency of skilled manpower, enhance pace of construction, implement environment friendly construction, ensure longer maintenance cycle etc. It is important that the technologies are conducive for use in extremely cold climatic conditions & high altitude areas required along India's Northern borders. Creation of Smart infrastructure to enable development needs to be linked to operational performance to provide clear and consistent direction to the industry on design and execution philosophy, cost saving mechanism and standardization of procedures could be adopted. It would facilitate in building of corporate knowledge, promote innovation and ensure speedy adoption of new technologies for development of smart infrastructure.

Streamlining Clearances

Land-acquisition and environment clearance processes continue to delay projects despite passing of a Land Acquisition, Rehabilitation and Resettlement Act (LARR) in 2013. The issues of long and difficult norms of obtaining permissions from the Ministry of Environment, Forest and Climate Change involving forested &environmentally sensitive border areas is resulting in cost & time over-runs of important projects. There is no intuitional mechanism for dispute resolution, impacting speedy execution of defence infrastructure projects. Hence, the provisions of LARR need to be reformed to speed up clearances related to defence infrastructure. Besides, the complex procedural issues of bureaucratic and inter-ministerial clearances also need to be smoothened to fast track the entire process of clearances.

Capacity Building and Asset Management

Evolution of holistic defence infrastructure development structures need to be planned by capacity building, formulating strategies, skill development, laying down responsibilities and incentivizing those who bring in efficiency and cost saving. Without clear lines of accountability it would be difficult to improve the performance of the organization in relation to infrastructure development and management plans. There is also a need to formulate legal provisions for stringent penalties against defaulters and a framework on defence asset management including data base in the form of eAsset and effective maintenance of course of action.

Conclusion

The state of the border infrastructure is a symptom of the larger security problems of India. The security scenario of the Country has changed significantly and the Armed forces need to adapt to these changes to meet current and future strategic requirements. The infrastructure strategies need to be visionary, realistic and relational with respect to financial policies, security dynamics, and other relevant influences . The strategic plans and initiatives need to identify issues affecting the defence infrastructure needs. The gap in the current planning philosophy and the future strategic direction needs to be bridged. Considering the security challenges facing the nation, there is a need to optimize the strategic balance between the infrastructure requirements and other military capabilities viz., personnel and equipment. The current approach to infrastructure development is to align the requirements with available resources in order to meet Government targets and budget allocation; however, the more appropriate methodology would be to formulate a long term plan for achievement of its strategic goals with relevant prioritizing of schemes. This can be done by identifying the optimal requirements of infrastructure and plan for its funding arrangements and delivery mechanism in a time bound manner. Well-developed defence infrastructure and other assets upto the border areas would supplement India's vision of becoming a regional power with greater economic engagement with its neighbors.

References

- *K. NarindarJetli and Vishal Sethi, "Infrastructure Development in India :Post Liberalisation Initiatives and Challenges,"New Century Publications, New Delhi, 2012.*
- *"Measuring National Power in the Post industrial Age," RAND Corporation Report, 2000.*
- *Monika Chansoria, "China's Infrastructure Development in Tibet", Manekshaw, Paper No 32, 2011.*
- *Dr. SubhashKapila, "China's Infrastructure Development in the Western Regions: Strategic Implications", South Asia Analysis Group, 2001.*
- *Antonio Estache and GrégoireGarsous, 'The impact of infrastructure on growth in developing countries', IFC Economics Notes, Note 1, April 2012.*
- *Annual Report to Congress, 'Military and Security Developments Involving the People's Republic of China,'Report of the Secretary of Defense, May 2016.*
- *Venkataramakrishnan, "Think-Tank Warns Lack of Infrastructure on Chinese Border Could Have 'Serious Consequences' for India", Mail Online India, 2013.*
- *Menon, J., and P. G. Warr, Does Road Improvement Reduce Poverty? A General Equilibrium Analysis for Lao PDR,In Infrastructure and Trade in Asia, edited by D. Brooks and J. Menon. Cheltenham: Edward Elgar, 2008.*
- *Guild, R., Infrastructure for the Pacific: Prospects and Challenges for Regional Cooperation, Paper presented at the inception workshop for ADB/ ADBI Flagship Study: Infrastructure and Regional Cooperation, 18–20 February, Tokyo, ADBI, 2008.*
- *Fujimura, M., Economic Integration in the GMS and Cross-Border Transport Infrastructure, Paper presented at the International Workshop on GMS Economic Corridors: Cooperation and Development, Yunnan University, 2008.*
- *Economic Research Institute for ASEAN and East Asia, Developing a Roadmap toward East Asian Economic Integration, ERIA Tokyo Forum, 2008.*

- *U.S. Army Peacekeeping and Stability Operations Institute, Infrastructure Reconstruction: Imperative in the National Interest, 2011.*
- *"The Times of india," 'Def Min wants Non-lapsable Capital Fund,' Aug 2017.*
- *Lok Sabha: Budget 2022-23, "Agreed to 15th Finance Commission's suggestion on non-lapsable Defence Fund: Finance Minister", Feb 2022.*
- *Gen V. P. Malik & Brig GurmeetKanwal, Defence Planning in India, ORF Institute of Security Studies, 2005.*
- *Department of Homeland Security, Critical Infrastructure and Key Resources, 2009.*
- *Ravi Mittal – "Private Participation in Infrastructure Sector in India". Published in YOJANA a Development, 2009.*
- *AmlanjyotiGoswami, "Land Acquisition, resettlement and Resettlement: Law and Politics," India Urban Conference, 2011.*
- *"The Diplomat," 'India Is Still Losing to China in the Border Infrastructure War, A year after the Doklam crisis, New Delhi faces the same old challenges in this realm,' Sep 2018.*
- *Peter Paret, "Military Power," The Journal of Military History, Vol. 53, No. 3, 1989.*

ABOUT THE AUTHOR

**COL
YOGESH NAIR**

Colonel Yogesh Nair, a 1994 Batch officer from the Corps of Engineers ia an alumni of Indian Military Academy and the Defence Services Staff College Wellington. Academically, the officer has a Masters in Civil Engineering, M Phil in Strategic Studies, and a PhD in Political Science. He has published numerous articles on defence and strategic issues in various journals. He is currently serving as Colonel Administration at the College of Military Engineering, Pune.

WAR IN UKRAINE – PART 2

BY AIR MARSHAL ANIL TRIKHA (RETD)

Current Situation

The War in Ukraine in its eighth month now, has clearly not gone the Russian way. The expectation that might of Russian arms would steamroll over Ukraine and force its capitulation in a matter of weeks has turned out to be more than a bit far-fetched. Emboldened by a steady stream of highly effective weapons from the West (mainly from the United States), Ukrainians have succeeded not only in halting the momentum of Russian advances but also gained a degree of psychological ascendance in the ongoing war of perceptions by inflicting some highly visible and effective attacks on high value Russian targets. On 14th April 22 Russia lost its Black Sea flagship – Slava class Missile Cruiser Moskva. Warring sides differ on what caused the loss of the ship. While Russians blame it to an onboard fire leading to explosion of ammunition, Ukrainians claim that it had struck the ship with indigenously developed 'Neptune' anti ship missile. The missile had reported been designed and developed by Ukrainian military engineers in response to the growing perception of threat from Russia's Black Sea fleet since the annexation of Crimea in 2014. The ship was equipped with triple tiered air defence system which if operating as designed, should have been able to defeat the attack. On 9th August, in another spectacular attack Russian airbase at Saky in Crimea suffered a major missile strike resulting in explosion of fuel/ammunition storage dumps and loss of a number of aircraft on the ground. Devastating attack on a base located 200 Km from the nearest frontline served notice that Ukraine had come to possess the ability to conduct precision strikes on strategic targets located in depth. The airfield is reported to have been protected by a multilayered air defense system including state of the art S-400 and Tor short range missiles. That the incoming missiles could pierce the defenses and cause extensive damage puts a question mark on Russia's ability to protect its high value assets in the conflict zone.

As of middle of September, Ukrainian forces appear to have launched an effective counteroffensive in the Kharkiv oblast and wrested back some 6000

Km of territory from Russian control. The forced retreat marks one of the most serious setbacks since Russian forces were repelled from the vicinity of Kyiv in the earliest days of the seven month old war.

The momentum of advance having been halted by Ukrainian resistance, Russians is now stretched thin along several miles long defensive line in East and South Ukraine. Assisted by Western intelligence identifying soft spots along this stretched frontier, it is entirely possible that Ukrainian forces would punch through Russian defenses in more areas. Although it is too early to write an obituary to the Russian offensive, there are signs that its human and material resources are stretched thin. Reports that North Korea may be helping replenish Russia's depleting Surface to Surface Missile stocks and Iran is pitching in with drones are likely early pointers to Russia's growing difficulties. On 21st Sep, Russia announced mobilization of 300,000 reservists to beef up its defences – some of them depleted by eight months of war. In an environment struggling to celebrate some success on the battlefield, it would be a tough call to enthuse fresh inductees to fight a determined opposition. In any case the commonly held perception of a powerful Russian military which could brush aside even first rate Western military forces in an offensive in Europe has been severely dented.

Warfare by other Means

Simultaneous to a shooting war on the killing fields of Ukraine, a wider economic political and information war is being waged both by Russia as well as Western powers supporting Ukraine. Carefully crafted mass media imagery of civilian casualties caused by unprovoked attack on a peaceful neighbor is eliciting widespread public sympathy for Ukraine. Led by the United States, the West has imposed wide ranging economic sanctions to isolate Russia from t the global market place and to inflict maximum possible pain. However, much to their frustration Russian economy has thus far withstood the pressure. India and China has continued to buy large quantities of Russian oil at discounted prices. Russian Ruble which had plummeted to 150 to US dollar in March has clawed its way back to 60/USD. But that is not to say that Russian economy can survive the crippling Western sanctions and prosper in the medium to long term. The Ruble is afloat mainly on oil and gas revenues. To choke this source of income, on 2nd September finance ministers of G7 countries comprising the US, Canada, the UK, France, Germany, Italy, Japan and the EU announced their intention to impose a price cap on the price of Russian oil at or below

which importers may buy. Failure to comply would attract a comprehensive ban on all services (viz. insurance, currency payment, facilitation and vessel clearances) which enable maritime transportation of Russian Oil and petroleum products globally. In retaliation for Western support to Ukraine Russia had already been squeezing the gas spigot to keep Europe on a tight leash. Coming in the wake of pandemic induced economic slowdown, soaring gas prices were hitting the consumers hard and warnings of a bleak freezing winter were ominous. Then in a tit for tat response to the G7 finance ministers 2nd September announcement of 'price cap', Russia cut off all gas supplies via Nordstream 1 pipeline. There being no alternative equivalent source of energy supplies, European economies built on a steady supply of cheap Russian oil and gas are likely to go into recession with all the attendant social and political consequences.

Both Europe and Russia are deeply mired in a high stakes game of poker hoping that the other side would blink first. It is therefore as much a battle of nerves as of resources (human and material) which may determine the final outcome. United States, the principal cheer leader of the confrontation against Russia is relatively immune to the short term fluctuation of fortunes of either side. In its reckoning the longer the war continues, the more it would erode Russian power thus enabling it to concentrate its focus on the Chinese challenge.

Russia's Geopolitical Compulsions

There is no doubt that Russia would have been aware of the dangers before deciding to launch its military operations in Ukraine and the larger game plan of the Western response. However its geopolitical compulsions are such that it could not have tolerated Ukraine drifting away to the Western camp. In his book 'Prisoners of Geography', Tim Marshall observes "Geography has always been a prison of sorts – one that defines what a nation is or can be, and one from which world leaders have often struggled to break free." Russia presents one of the most striking examples of how geography has influenced its choices and history.

In the vast geography of Russia covering 11 time zones, Ural Mountains stretching a thousand miles from North to South constitute both a notional as well as a physical barrier between European and Asian Russia. European part occupies a quarter of the area but is home to more than three quarter of Russian population. It is Russia's political and cultural heartland which defines

the Russian nation. While this core is well protected by mostly frozen Arctic Ocean to the North and vast Siberian expanse to the East, the most serious vulnerability of the heartland lies in the colossal Northern European plain on Russia's West. Stretching from Baltic Sea in the North to the Carpathian Mountains in the South encompassing all of Western and Northern France, Belgium, the Netherlands, northern Germany and nearly all of Poland, this vast stretch of flat land is ideal terrain for armies to roll down deep into the Russian heartland. In the past 500 years Russia has suffered invasions from the West several times. Poles came across the North European plain in 1605. The Swedes followed in 1708. Napoleon in 1812 and Germans in both World wars in 1914 and 1941. If Crimean war of 1853-56 is included amongst the invasions, then starting from Napoleon's invasion of 1812, Russians have been fighting in or around the North European plains every 33 years. The narrowest 300 mile wide gap (between Russian exclave of Kaliningrad to the North and Carpathian Mountains to the South) lies in Poland., Thereafter the wedge begins to broaden until presenting a 2000 Km wide frontage at the Russian heartland - making it extremely difficult to defend.

At the end of WWII in 1945, Russia occupied territory conquered from Germany in Central and Eastern Europe. Some of occupied territory became a part of the USSR while the remaining countries such as Romania, Hungary,

Czechoslovakia, and Poland were pulled into the Soviet orbit as satellite states. The Iron Curtain served as a robust buffer zone protecting the Russian heartland and threat of 'Mutual Assured Destructive' helped maintain a cold peace and frozen frontiers. With the end of the Cold War and Soviet Union's collapse, there was a glimmer of hope that political winds would also change and old antagonisms reminiscent of the Cold War may give way to a more accommodative order between the West and Russia.

As a hopeful sign of a change, formal contacts between NATO and Russia began in 1991 itself within the framework of the North Atlantic Cooperation Council (later re-named Euro-Atlantic Partnership Council). In June 1994 Russia became the first country to join NATO's Partnership for Peace (PFP) program of practical bilateral cooperation between NATO and states of the former Soviet Union. Even Vladimir Putin (the current bête noire of the West) had articulated a vision of a flourishing Greater Europe and a common economic space from Lisbon to Vladivostok. The principal idea underlying the PFP initiative was to incentivize a cultural shift in the mindset of states once behind the Iron Curtain without alarming Russia. However within less than a year of launching the PFP, Clinton administration in a reversal of policy introduced the goal of NATO expansion. The stated reason was that instability in Central and Eastern Europe had led to two great wars in the 20th century. By drawing states of the region into the alliance would eliminate a potentially destabilizing power vacuum in Europe. What remained publically unsaid was that the enlargement was also to serve as a hedge against the possibility of Russia reasserting its control over its erstwhile satellite states in Eastern Europe. Russia's sense of security began to unravel as the former communist states on its periphery began to gravitate towards the West. Russia's own efforts to integrate itself in the Western liberal framework through PFF like mechanisms proved stillborn and Russia was too weak and distracted by internal turmoil to influence the trajectory of states which had acted as a buffer since the end of WWII.

In its euphoria of triumph following the Cold War, West let go of the unwritten understanding of not expanding NATO any further East than where it was at the time of German reunification. NATO's remorseless expansion began in 1999 when Poland, the Czech Republic, and Hungary became member states, followed by the Baltic States, Bulgaria, Slovakia, Slovenia, and Romania in 2004. Albania and Croatia joined in 2009, while Montenegro and Macedonia fell in NATO's fold in 2017 and 2020 respectively. Poland and Rumania now house US installed Ballistic Missile Defense systems. This gives rise to the possibility of a build up of missile network in Europe which could undermine Russia's first or second strike capability - thus seriously eroding its deterrence against NATO

threat emanating from the North European Plain. Historical memory of past invasions from this direction evokes Russian paranoia of an existential threat materializing once again on its borders

Importance of Ukraine

Ukraine was one of the founding republics of erstwhile USSR and even after the latter's dissolution in 1991, and it becoming an independent republic it remained a key buffer state on Russia's periphery. When Ukraine began to teeter into the EU orbit by way of the Association agreement – a step toward EU membership, and perhaps a few away from joining NATO, Russia sensed an existential threat developing on its borders. Western argument that neither EU is a military alliance nor NATO an offensive one does not cut any ice with the Russians. Its anxieties about change of Ukrainian loyalties also lay in the enormous geopolitical significance of the Crimean Peninsula which is home to the Russian Black Sea Fleet (BSF) at Sevastopol. BSF though constrained by narrow outlet from the Black Sea, is vital to Russia for its power projection capability in the Atlantic Ocean. The Sevestopol lease arrangement between Russia and independent Ukraine worked smoothly until outbreak of the Maidan revolution and open Western encouragement for Ukraine to shake itself of its pro-Russian moorings. To ward off the emerging threat, in 2014 Russia moved swiftly to annex Crimea. In retaliation, West applied a slew of sanctions. Geopolitical tensions escalated rapidly with both sides moving to solidify respective advantage.

NATO is a collective security organization. The crux of its substance lies in Article 5 of the Treaty, which explicitly states that "an armed attack against one or more of the member states shall be considered an attack against all." This implies that if Ukraine joined NATO and if it ever felt threatened, US and allies would be treaty bound to defend it. It would have also opened the possibility of US and its NATO allies deploying bases, forces and even lethal weapons on Russia's sensitive border. This was an intolerable threat which Russia could not ignore. Russia's gambled to scotch the looming threat with a quick military assault aimed at the heart of Ukrainian rebellion. What followed has now become a part of history.

Sweden and Finland's Application to Join NATO

On the Northern edge of Europe both Sweden and Finland have been working closely with NATO since the end of the Cold War, and had participated in close conjunction with NATO forces in the Balkans, Afghanistan, Iraq and Libya. Armed forces of both have adopted NATO's 'Standard Operating Procedures' which facilitates easy interoperability in a crisis. Their membership of UK's Joint Expeditionary Forces which has eight other NATO members is indicative of their proximity to the Alliance. However despite their pro-Western political orientation and even close military liaison, throughout the Cold War both Sweden and Finland remained steadfast in their publically supported neutral stance between the West and Russia. This began to shift after Russian forces annexed Crimea in 2014. Following the Russian invasion of Ukraine in February 2022, public opinion in both countries has tilted decisively in favor of a formal alliance with the West. In May 22 both Sweden and Finland applied for membership of NATO.

Sweden, as a symbol of its national identity has historically been opposed to military alliances and has carefully navigated its way avoiding military entanglements for over 200 years. It fought its last war in 1814 against its neighbor Norway. Since the end of the Cold War, its foreign policy was largely focused on multilateral dialogue and nuclear disarmament. Feeling safe and secure in the then prevailing world order, in the 1990s it reduced the size of its military substantially and prioritized peacekeeping missions around the world over territorial defense. All that changed in 2014 when Russia annexed Crimea. Conscription abolished in 2010 after being in vogue for nearly 110 years was reintroduced, and defense spending increased substantially. Subsequent Russian activity in Sweden's proximity has heightened Swedish concern. There have been reports of air space violations of Swedish airspace by Russian military aircraft and a submarine was suspected to have been prowling around in the shallow waters of Stockholm archipelago. Alarmed by the rapidly worsening security scenario, Swedish army reoccupied Gotland, (the strategically important Baltic Sea Island) after having abandoned it two decades ago. To emphasize reversal of its traditional neutral stance in East West confrontations, three days after Russia's invasion, it sent military assistance to Ukraine including 5000 anti tank weapons.

Until 1992 Finland's relations with Russia (successor state to the USSR) were governed by a political treaty signed in 1948. It limited Finland's role in Western Europe and obliged it to help defend The Soviet Union if it ever felt

threatened. The treaty effectively ruled out Finland's membership of European Community and gave rise to the term 'Finalandization' to describe a weak country accommodating itself to a strong one in order to maintain its autonomy. In the changed political environment following the collapse of Soviet Union, Finland stepped out of Russia's shadow and joined the European Union in 1995. However the idea of joining NATO remained dormant, rooted in public belief that while robust political, economic and even military relations with Western powers were extremely beneficial, peace was best kept by simultaneously maintaining friendly relations and economic ties with Russia also. Even after Russian annexation of Crimea, Finland reacted very cautiously and ensured that lines of communication with Russia remained open. While expressing its indignation at Russia's military action, it did not formally abandon its policy of neutrality. The penny dropped when Russia invaded Ukraine in Feb 22. Finnish perceptions changed dramatically. In early 2022 public opinion polls in Finland had found only 24% of the public supported NATO membership. Four days after the invasion the number in favor jumped to 68%.

Sweden and Finland's application for NATO membership has to be unanimously approved by all 28 NATO member states and ratified by US Senate. Indications are that it is only a matter of time before both countries are formally admitted to the alliance. Although relatively small in population (Finland 5.6 million, Sweden 10.24million) both Finland and Sweden have very competent and well equipped militaries which would be net security assets to NATO in Northern Europe.

Finland's Air Force has 64 X F-18 fighters with 'smart weapons' bought from the US in 1992 and a further 64 state of the art F-35s are on order –supplies commencing in 2026. Its seriousness about defense of its homeland is amply demonstrated by its extremely well organized civil defense apparatus, ready to go into crisis mode at short notice. Helsinki itself has 5000 bomb shelters fully equipped with food and other amenities. By law Finland is required to hold in reserve three months of imported prescription drugs, and six months of food and fuel. Polling data shows that 74 % Finns would be willing to fight for their country's independence – which is the highest amongst democracies.

Sweden maintains a relatively broad set of advanced capabilities supported by its large and sophisticated defense industry. On land this includes armored, mechanized, airborne, artillery and air defense units – the latter including state of the art 'Patriot' batteries. Swedish Air Force operates nearly 100 top of the line domestically produced Gripen multi role fighter aircraft. The Navy employs one of the most advanced domestically built submarines – the first non-nuclear submarine to feature an air-independent propulsion system.

Norway is already a part of NATO. Sweden and Finland's accession would bring all Arctic states except Russia into the Alliance. Russia has warned that while it doesn't object to this expansion, it would not tolerate NATO forces or equipment to be positioned in the region. Norway allows access to NATO allies for exercises but does not permit permanent installations or nuclear weapons on its territory. Swedes have also have stated that they don't want to host NATO assets permanently. Finland has yet to indicate its preferences.

Russia's Stake in NW Europe

Russia operates world's largest fleet of submarines from its Baltic seaports. On their way to the Atlantic Ocean, Russian subs sail outside the territorial waters of the Baltic States to reach Danish straits. Free passage through Baltic is the only way for Russian submarines to evade US undersea sonars. Finland and Sweden's accession to NATO would potentially turn the Baltic into a NATO lake which would render it virtually impossible for Russian submarines to negotiate the narrow passage undetected. Finland's accession to NATO also carries most serious implications for Russia's strategic posture. Severomorsk located at the northern edge of Kola Peninsula (adjacent to Finland) is home to Russia's powerful Northern Fleet. Unlike the rest of the arctic, this coastline is warmed by the Gulf Stream which keeps it ice-free throughout the year – a natural phenomenon which enables modern nuclear and diesel submarines constituting Russia's second strike nuclear capability to maintain a high degree of readiness to respond to any crisis. Nearby Plesetsk cosmodrome is home to Russia's Topol M/RS 24 ICBMs with range of 11000 Km. Western part of the peninsula is densely packed with Russian strategic forces with a number of airbases hosting TU 116M, TU 124 and TU 95 bombers. Therefore Russian forces in the Kola Peninsula constitute the crux of Russia's power projection capability. As climate change opens up the arctic passage, facilities in Kola will become even more integral to Moscow's strategic posture. Finland's accession to NATO will more than double Russia's border with the Alliance, the defense of which will impose an exorbitant economic burden on Russian resources. A single parallel 700 Km long road / rail link is the main communication artery between Murmansk on the Northern tip of the Kola Peninsula with St.Petersburg and Moscow. All firepower, deterrence, and power projection capabilities are concentrated along this single axis. The area is covered by thick pine forest which makes it especially suitable for Special Forces' operations. With the potential of threat

developing at short notice at any point along this long corridor, defending it would be extremely costly and resource intensive.

Russian Retaliation

Russia has for years warned that it would take military steps, to counter Finland and Sweden's decision to join NATO. Former President and currently deputy chair of the Russian National Security Council, Dmitry Medvedev openly threatened that Russia would consider deployment of nuclear weapons and hypersonic missiles in its Kaliningrad exclave. Very mention of nuclear weapons being extremely provocative, President Putin pulled back a step quickly by changing the narrative. Addressing Summit Conference of the 'Collective Security Treaty Organization' on 16th May, he declared that expansion [of the alliance] with these countries does not pose an immediate threat to Russia." Russia's concern, he said, would be what "military infrastructure" the alliance deploys in the new member states.

Besides threatening fresh nuclear deployments in response to NATO's expansion into Norway and Sweden, Russia has some other retaliatory options too. It could launch a pincer from its exclave Kaliningrad in the North West and Belarus in the South East to close the 40 mile gap along the Lithuanian Polish border. This would effectively cut off the Baltic States (Latvia, Estonia and Lithuania) from the EU. It could also terminate lease on the canal linking Lake Saimaa in Finland to European markets thus hurting Finnish exports. Notwithstanding these possibilities, given Russia's problems related to its military commitments in Ukraine, for now Russia's response is likely to remain limited to economic and political actions alone. However deployment of NATO bases, troops and weapons on Finland's soil will serve to raise the hair trigger environment developing in Russia's confrontation with the West.

Conclusion

Chastened by failure of predictions of early Russian victory, it is difficult to hazard a guess about how the current conflict may end. In the still developing story, Russia has upped the ante by ordering mobilization of 300.000 reservists and threatening to take all measures to achieve its politico-military objectives. West's warnings of staying the course to thwart Russia are equally ominous.

Vast geography and endowment of abundant natural resources gives

Russia both the potential of being a great power as well as a lucrative prize. Its weakness lies in its geography. While to the North and East it is well protected by natural features, its heartland is dangerously exposed to the vast North European Plain. Repeated invasions from the West have imprinted a historical memory on the Russian psyche and evokes paranoia about any potential threat from that direction. To minimize the danger, Russia would ideally like to push West and anchor its defenses on the more manageable gap between the Baltic to the North and the Carpathian Mountains to the South. That space lies in Poland, which after dissolution of the Warsaw Pact is out to seek revenge for its own grievances against Russia.

Ukraine's drift towards the EU with an aspiration to finally join NATO would have exacerbated Russia's geopolitical problem several fold. It could have been dispossessed of Crimea and with it Sevastopol – the home of its Black Sea Fleet. With Poland already staunchly embedded in NATO, the flatlands of Ukraine would have extended the flat North European all the way to the sensitive Volgograd gap thus creating the possibility of severing Russia from its Southern Republics and access to the Caspian Sea. It is therefore no surprise that Ukraine's political orientation is crucial to Russia's security.

If security against expanding NATO was at the heart of Russia's reason for invading Ukraine, then its overall security situation has deteriorated even further. With tenacious resistance to the invasion, Ukrainians have discovered a strong belief in their national identity, thus laying to rest (perhaps permanently) Russia's claim of a fraternal relationship and source of the problem only being a delinquent regime seduced by Western propaganda. Accession of Finland and Sweden to NATO will only add another dimension to Russia's insecurity.

Ukraine's war effort is supported by Western (US and European) arms and vastly greater resources. Russia, perhaps with some support from North Korea and Iran, is in the fight mostly on its own. If China were to be in support of Russia, it could have balanced the equation to an extent. However despite declaration of 'No Limits Partnership' and their shared interest in checking overweening US power, China has limited itself to only political and diplomatic support – carefully avoiding any action which may attract the weight of secondary sanctions of the Western block. Given the balance of forces, outright victory of neither side looks likely. Therefore at some undetermined stage in future, perhaps due to exhaustion, some manner of peace agreement may be negotiated. However that is unlikely to resolve Russia's problem bequeathed by its geography.

What sort of a world is likely to emerge after this war? Whatever the other outcomes, Russia is likely to be much diminished. A weakened, humiliated and

insecure Russia shunned by Western powers and with a weakened economy, is likely to become beholden to China. With its nuclear arsenal intact and simmering grievances, it is likely to make common cause with China in a robust push back against Western interests globally. Suffering in wake of the pandemic and economic recession brought about by soaring energy costs, Europe is likely to see a surge of right wing populism. Ripple effects of what is happening at the Eastern edge of Europe will be felt all across the world. India has thus far hedged its bets by staying neutral. However historical memory of support at critical junctures and deeply embedded defense equipment dependence on Russia on the one hand, and increasing bonhomie with the US on the other under the shadow of growing power and assertiveness of China, is likely to compel it to make some hard policy choices.

References

- *What is the G7 planning on Russian Oil - The Hindu Sep 11,2022)*
- *https://www.bbc.com/news/world-europe-61397478.amp*
- *https://www.usip.org/publications/2022/06/russia-has-relaxed-its-rhetoric-natos-nordic-expansion*

ABOUT THE AUTHOR

**AIR MARSHAL
ANIL TRIKHA (RETD)**

Air Marshal Anil Trikha (Retd) Was Commandant of College of Warfare at Secunderabad, Air Defence Commander South Western Air Command ,Commandant National Defence Academy and AOC-in-C Southern Air Command. After retirement, appointed Chair Professor of 'Air Power and National Security Studies' in the 'National Institute of Defence Studies and Analysis' at the University of Pune until Sep 07. Now writes on Strategic Affairs in various journals and newspapers and delivers lectures occasionally at different institutions.

INTELLIGENCE – THE FIRST LINE OF DEFENCE

BY REAR ADMIRAL RJ NADKARNI AVSM VSM (RETD)

Introduction

The history of intelligence is perhaps almost as old as warfare itself. Since the earliest days, leaders and military men have known about the importance of intelligence in the conduct of a campaign. For some, intelligence has always had a certain notoriety due to its close association with spies and traitors like Kim Philby and Oleg Penkovsky. For others, influenced by the exploits of James Bond, spies mean a life of glamour, adventure and romance. Yet, intelligence is for the most part a rather laborious, dull and thankless affair whose functionaries live a rather ordinary and anonymous life.

Intelligence has three main components: information gathering, analysis and dissemination, aimed at providing the leadership and policy makers better inputs on taking important decisions. Intelligence can be strategic, operational or tactical. While strategic intelligence would be required more at the level of the political leadership, operational and tactical intelligence would be required by military commanders at these respective levels of warfare.

Broadly speaking, intelligence is about knowing more about the enemy's capabilities and intentions. Collection of intelligence on a potential adversary's capabilities is a fairly simple concept even if it is not especially easy for the agency doing the collection. On the other hand, trying to assess an adversary's intentions is much more difficult to predict and imprecise. This is the reason why intelligence agencies have often failed to connect the dots and realised their lapses only in hindsight.

Till the 19th century, intelligence gathering was mostly the realm of spies and agents. This is now referred to as Human Intelligence (HUMINT) and continues to be an important component of intelligence overall. However, as technology has progressed, several more disciplines such as Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Measurement and Signature Intelligence (MASINT), Technical Intelligence (TECHINT) and Counter Intelligence (CI)[1]

have evolved. While most intelligence gathering is either covert or beyond the adversary's capability to deny e.g. satellite photographs, Open Source Intelligence (OSINT) relies on information freely available in the open domain, typically obtained from newspapers, TV channels, websites and other media sources.[2]

A political leader requires intelligence about a potential adversary nation's capabilities to assess funding required to develop his own armed forces capabilities, force structure and preparedness to deter any aggressive action by the latter. The military commander, on the other hand, needs sound intelligence to effectively carry out war fighting once hostilities have been declared. The disciplines of intelligence that rely on technology have reduced the so called 'fog of war' and enabled today's leaders and commanders to take quicker decisions as well as communicate them to lower formations.

Major Intelligence Failures in World War II

Even more important than knowing the enemy's capabilities is the assessment of his intentions, so as to take appropriate counter or deterrent actions. Throughout history, there are several instances where these intentions were either not accurately assessedor taken heed of and led to major world wars.

In 1941, the world witnessed two cataclysmic events which would change the course of history and reshape the geopolitical environment for the next 50 years. While they happened in diametrically opposite sides of the world, they both had one thing in common in that they were amongst the greatest intelligence failures of all time. These events transformed the war started by Adolf Hitler in September 1939 from one that was largely being fought in Western Europe to one that would encompass the entire globe. As you may have guessed, these were Operation 'Barbarossa' - the invasion of the Soviet Union by Germany on 22 June and the 'Day of Infamy' - the Japanese attack on the US Naval Base at Pearl Harbor on 07 December.

In autumn 1938, Britain and France looked on with concern as Germany annexed Austria and then threatened to invade Czechoslovakia. In September 1938, Germany, Britain and France signed the Munich Agreement, giving Germany the right to annex the Sudetenland, in return for it not invading Czechoslovakia. The hopes of British Prime Minister Neville Chamberlain – memorably shown waving a piece of paper signed by Hitler and proclaiming

'Peace in our time!'– were, however, doomed to turn to ashes when Germany reneged on the agreement by occupying Czechoslovakia itself in March 1939. This was followed by the infamous Molotov-Ribbentrop Pact Non-Aggression Pact between the Soviet Union and Germany on 23 August, followed by Hitler's invasion of Poland on 01 September, triggering the Second World War. While the Soviets believed the Pact to be inviolable, for Hitler it was only a means of gaining time to build up his military machine and also keep the Soviets from attacking him while he embarked on his war of expansion in Western Europe. Given his policy of 'lebensraum' or living space[3], it was another promise he never intended to keep[4]. The Soviets at the time had one of the most professional intelligence organisations in the world – the NKVD. They also had one of the most redoubtable double agents – Richard Sorge – working in the Nazi Embassy in Tokyo, but actually spying for the Soviets[5]. Sorge through his contacts in the Embassy sent numerous reports to the Kremlin in early 1941 about the Nazi designs to invade the Soviet Union[6]. Yet, Joseph Stalin in an act of self-delusion chose to ignore these warnings, even as more than 150 German divisions massed at his border[7]. When Operation Barbarossa was indeed launched on 22 June, Stalin is reported to have been dumbstruck and went into a depression[8].

On the other side of the world, relations between the Japanese Empire and the United States had also deteriorated, with the latter imposing severe trade sanctions, including on the import of oil. This created a very difficult situation for Japan, being dependent as it was for 95% of its resources[9]. Meanwhile, US intelligence had managed to crack the Japanese diplomatic cipher 'Purple' and was able to access messages that were being sent by the Japanese Government to its Embassy in Washington[10]. The 'Winds Code' were a set of instructions from Tokyo to Japanese embassies regarding the state of diplomatic relations with the US[11]. The message "East Wind Rain" would indicate an imminent breakdown of diplomatic relations with the United States. The Winds Code had in fact been deciphered by the Americans who were indeed expecting an attack by the Japanese. However, they assessed that this strike would be launched in South East Asia and had no idea that the intended target was Pearl Harbour. The Japanese Government also intended to make a formal declaration of war on the United States prior to the actual attack, and had sent the now famous '14-part message' to its Embassy in Washington to be handed over to the US Secretary of State, Cordell Hull at precisely 1 p.m (7a.m. in Hawaii)[12]. However, due to various reasons relating mainly to slow decryption and typing, the Embassy could only deliver it at about 2.58 p.m – about an hour after the attack had commenced[13]. Meanwhile, American code analysts had

already intercepted, and deciphered the 14 Part message, but did not connect the dots when it came to realising the significance of the time when it was to be handed over to the Secretary of State[14]. The Americans also did get several warning signs on the morning of 07 Dec itself, such as a large group of aircraft headed towards Pearl Harbour detected by an experimental radar installed on a mountain in the North of Oahu Island and a Japanese midget submarine being sighted at periscope depth off the harbour (and subsequently sunk). Yet the Americans failed to go up in alert state[15].

Intelligence Successes during World War II

To their credit, the Allied nations learnt their lessons well from these intelligence failures and later on had many victories over the Axis, with intelligence contributing a significant part. Along with the Japanese diplomatic code 'Purple,' American crypto analysts operating from Station Hypo at Pearl Harbour had partially cracked the Imperial Japanese Navy's JN-25 code and were aware that a major offensive operation was underfoot. The only question was about the intended target. The code referred to this target as "AF," but the identity of "AF" was a mystery. Commander Joseph Rochefort, the head of intelligence, believed this to be Midway. To confirm this, an uncoded (and dummy) radio message was transmitted by Midway saying that its water desalination plant had broken down. Soon thereafter, the IJN transmitted a message indicating that "AF was short on water." This allowed the C-in-C Pacific Fleet (CINCPAC), Admiral Chester Nimitz to deploy his task force in advance off Midway without the Japanese being aware of it[16]. While this in itself may not have been the single biggest factor in the American victory, there is little doubt that it played a very significant part as it gave them the initiative, which ultimately proved decisive.

On the other side of the world, German U-Boats using deadly wolf pack attacks were creating havoc in trying to choke Britain's seaborne trade. The British urgently needed to find ways and means to counter the U-boats. One of these methods involved decrypting communications between German Naval Headquarters and the U-Boats at sea. The messages were encrypted using a highly sophisticated (for its time) analogue crypto machine known as Enigma, which used a number of electro mechanical rotors. A motley, but brilliant, team of scientists, academicians and mathematicians assembled at a residential manor called Bletchley Park to work on cracking Enigma[17]. This team, known as Ultra was led by a mathematical genius Alan Turing, who was assisted by

Gordon Welchman. Team Ultra put in hours of back breaking work and through a process of trial and error was able to design a machine called 'Bombe' which could decrypt Enigma[18]. Later Ultra designed an even more sophisticated machine 'Colossus' now considered to be the world's first programmable digital electronic computer[19] to decrypt even more complex messages. The intelligence derived from Ultra proved invaluable in allowing the Allies to know of German U-Boat deployments, but was disseminated with discretion so as not to alert the Germans to the fact that Enigma had been compromised.

Intelligence Organisations

Today all the major world powers possess large, well equipped and professionally staffed intelligence agencies. The US has the Central Intelligence Agency, the UK has the Secret Intelligence Service or MI-6, Israel has Mossad, China has the Ministry of State Security (MSS), Pakistan has the Inter-Services Intelligence (ISI) and India the Research and Analysis Wing (R&AW). Each of these central intelligence agencies is supported by various other departments which provide military intelligence, IMINT, MASINT, SIGINT, ELINT, etc to specific consumers based on their roles and functions[20]. For example, the Intelligence Bureau of the Joint Staff Department is the military component of the MSS in China[21]. Many of these agencies are also authorised not just to collect intelligence, but also take proactive and often pre-emptive actions in countries that may be considered a threat, which may include targeted assassinations[22] such as the CIA led operation which led to the killing of Osama bin Laden[23] or to instigate regime changes such as the attempted overthrow of the Castro Government in Cuba during the failed Bay of Pigs invasion[24].

The ISI, while purportedly a military intelligence organisation, is also the premier institution that plans and executes Pakistan's proxy war with India[25]. In the past terrorists handled by the ISI have carried out major attacks in India such as the 2001 attack on the Indian Parliament in New Delhi[26] as well as the 2008 terror attacks in Mumbai[27]; both of which almost led to hostilities breaking out between the two nations.

While the ISI's main strength lies in HUMINT, countries such as the US and China have developed over the years a very sophisticated and well-developed system of collecting electronic intelligence to include SIGINT, ELINT and MASINT as well as an elaborate system of reconnaissance 'spy' satellites. This has resulted in almost total 'battlefield transparency' where almost any platform

of the adversary as well as troop and formation movements can be located and tracked in near real time.

The US National Security Agency is tasked with the responsibility of monitoring electronic communications (SIGINT) and also covers cyber security[28], thereby providing the political leadership and military commanders timely intelligence to warn of any threat to its national security whether from a conventional adversary or a terrorist group. The NSA has about 30,000 employees, but even they would not be able to continuously monitor the humongous amount of communications traffic taking place every single minute. For that, the NSA employs a number of supercomputers, each of which uses complex algorithms and a number of keywords as well as Artificial Intelligence, all of which is able to 'red flag' communications which then are further processed by the human analysts to decide whether a particular communication comprises a threat or is harmless[29].

The Third Department of the PLA General Staff Department is China's premier cryptologic service[30] with specific missions, such as radio or satellite communications interception. While there are few accurate sources which list details of this organisation, it is believed to have around 130,000 analysts performing similar tasks as that done by the NSA[31].

The Research and Analysis Wing (R&AW) is the foreign intelligence agency of India. The agency's primary function is gathering foreign intelligence, counter-terrorism, counter-proliferation, advising Indian policymakers, and advancing India's strategic interests. The head of R&AW is designated as the Secretary (Research) in the Cabinet Secretariat, and is placed directly under the PMO[32]. In addition, all three Services have their own intelligence organisations, which get inputs from various sources including the R&AW and disseminate it to lower formations.There is also the Tri-Service Defence Intelligence Agency (DIA) under the IDS which synergises the efforts of the int agencies of the three Services. It also coordinates with other national agencies involved in gathering intelligence to provide intelligence support to the Armed Forces[33].

The National Technical Research Organisation (NTRO) is the technical intelligence agency of the Govt of India, which comes under the NSA and is part of the PMO. The agency specialises in multiple disciplines, which include remote sensing, data gathering and processing, cyber security, geospatial information gathering, cryptology, strategic hardware and software development and strategic monitoring[34].

Requirements of Intelligence Organisations

Most of the intelligence organisations mentioned earlier have a set of highly professional and skilled staff, comprising both operatives as well as analysts. Other than a few high-ranking officials, most of the staff remain anonymous, unless they suddenly turn whistle-blowers as in the case of Edward Snowden[35]. Funding for intelligence agencies is rarely revealed publicly, but needs to be a substantial amount to cater for operating, managing and maintaining all the technical assets, payment of sources or operatives as well as salaries of the thousands of analysts that work for the organisation[36].

Operatives and double agents working inside the target country would be expected to pass off as a local and hence must possess faultless language (and accent) skills and complete knowledge about its culture and society[37]. OSINT analysts too would need to possess good language skills, to analyse inputs in the local language[38]. Most intelligence will be disseminated on a need-to-know basis, depending on the designation, status, roles and responsibilities and authority of the recipient.

Persons to whom such intelligence is passed are expected to exercise utmost discretion and not reveal it to others down the chain, unless essential for the latter's' functioning. Most intelligence collection methods need to have plausible deniability, lest they end up proving to be a major embarrassment to the nation and organisation employing them[39]. These apply specially to cultivated sources and operatives deployed in target countries, if they are exposed by the counter intelligence organisations of those countries.

Nations which employ such methods also display ruthlessness in their actions, which may or may not go hand in hand with their professed national ideals such as freedom, justice, equality, etc but are undertaken nevertheless as they are considered to be "in the national interests." On occasion, intelligence agencies set up primarily to target other countries, have also been tasked by the Government to spy on their own citizens as the Edward Snowden incident revealed.

Technological Advances

Following the Second World War, the world has seen several new technological advances in the field of intelligence collection, of which the two most significant ones are the advent of satellites and computers.

Satellites can enable a range of functions, of which the most important are communications, navigation and remote sensing, with reconnaissance (spy) satellites essentially being the last named. These satellites allow powerful nations to keep an eye on areas of interest, whether they be on land or at sea. Spy satellites can be of various types depending on the type of sensor (optical, radar or ELINT) and orbital pattern (geostationary, polar or elliptical)[40]. Each has its own advantages and is therefore deployed for a very narrow and specific purpose. For example, low earth orbit satellites can only photograph a narrow band of land area along the path that they are orbiting (known as the swath). This makes them suitable for carrying out surveillance of, say,army formations with a very high resolution, but not for maritime surveillance for which the satellite has to cover a very large area. This can only be done by a geostationary satellite i.e., one whose orbit exactly matches the Earth's rotational speed and path[41]. Unlike high flying, fast reconnaissance aircraft, which most major powers used extensively during the latter part of the 20th Century, satellites cannot be intercepted in peace time as they orbit above the atmosphere and are consequently outside the airspace of a nation. However, they can be intercepted and destroyed during hostilities by anti-satellite missiles[42]. They can also be electronically jammed or blinded by high energy lasers to deny the country operating them access to their information[43].

The other major technological advance in the field of intelligence gathering has been in the field of computing. From the days of the Bombe and the Colossus, computers have come a long way and presently have a tremendous amount of computing power. This gives rich and powerful nations such as the United States and China the capability to monitor and analyse all types of communications whether through radio, telephone lines, mobile networks and the Internet in near real time. The next step in computing technology will be the transition to quantum computers and much research into these next generation machines is presently taking place. Quantum computers promise processing power of a magnitude that would make today's supercomputers appear to crawl in comparison. When data to is analysed protected by a secure key or password, the time taken to crack it – using a technique known as 'brute force attack' – is exponentially proportional to its length and complexity. Quantum computers are expected to significantly reduce this time taken, thereby enabling a quicker response[44].

The recent entry of the Chinese ballistic missile and satellite tracking ship, 'Yuan Wang 5' into Colombo Harbour, caused some degree of consternation in Indian strategic and policy making circles. However, the use of intelligence collection ships is an old practice, employed by several countries for decades

including the United States, erstwhile Soviet Union[45] and the present-day China. These ships masquerade as survey, research, scientific or even innocuous fishing vessels, but carry sophisticated equipment to monitor electronic transmissions emanating from the target country[46]. International Maritime Law permits such vessels to travel to as close as 12 miles from the target country, that being the limit of its Territorial Waters.

In addition to signals transmitted through the airwaves, there are a number of vessels which also carry underwater sensors which can monitor the hydrological and bathymetric conditions prevailing in a particular part of the ocean. This data is of utmost importance for detection of submarines by surface ships and aircraft. The primary sensor used by these platforms - the sonar - depends on sound energy reflecting off the hull of a submarine to detect it. However, sound does not generally travel in a straight line underwater but is affected by the changes in temperature, pressure and salinity with depth. Consequently, knowledge of these conditions in advance can enable a submarine to remain at a certain depth below the surface, where a surface ship will be unable to detect it. Over the past few decades, the incidents of Chinese 'research vessels' - which are believed to carry such underwater sensors – have increased in both the South China as well as the Indian Ocean[47]. China also has thousands of fishing vessels, commonly referred to as its 'Maritime Militia, employed in a dual role for collecting intelligence[48]. The problem with identifying such vessels is that their sensors, being underwater, are hidden from view. Hence an investigating ship will have to board the suspect vessel to confirm that it is in fact recording ocean data, which is a risk when carried out in international waters since it may lead to a diplomatic incident.

Actionable Intelligence

The key inputs that the political leadership and military commanders desire more than any other can be termed as 'actionable intelligence.' In simple terms, this means one or more'what', 'where', 'when' and 'how' component of an event of significance, which could be something as momentous as an invasion of another country such as Operation Barbarossa or a terrorist attack on a prime target. Intelligence obtained through technical assets may not be able to reveal all the inputs that the leader or commander may desire. Hence, HUMINT still remains an invaluable and often more accurate source of information that can be used to plan a response. For example, US operations to target and kill Osama bin Laden[49] and Al Zawahiri made use of multiple sources

of intelligence to confirm their target location and behavioural pattern before carrying out their successful attacks. Providing such actionable intelligence is always a balancing act for agencies. They need to ensure that all valid inputs are disseminated, but at the same time be alive to the 'Cry Wolf' syndrome, which is when too many false positive inputs are disseminated. These could lull the recipient into a sense of complacency and not respond in time when an actual threat materialises.

Defence Attaches

Defence Attaches who are posted to Embassies of their country are also a source of intelligence; though due to their diplomatic status, they can only glean information through overt methods. Several countries employ trained intelligence officers as Defence Attaches. These officers – and their families - undergo a special course to acquaint them with the culture, society and language of the country in which they will be posted[50]. Such information can be invaluable during informal gatherings when the Attaché can pick up bits and pieces of conversation that the locals may be speaking in their own language – perhaps lulled into a false sense of security by the belief that the Attaché does not understand them, when in fact he does.

The Future of Military Intelligence

Two cutting edge technologies that major powers are investing vast sums of money in are Artificial Intelligence and Unmanned Autonomous Vehicles (or Vessels). Both of these technologies, as they mature, are expected to reduce – if not completely eliminate – the human element presently required to conduct various aspects of warfare, including intelligence collection and analysis. With the incorporation of these technologies, intelligence inputs are like to be more accurate, analysed and disseminated faster. These systems can also work 24 x 7 at full efficiency without the need to take biological necessity breaks as human operators would have to. Unmanned aerial or underwater drones could stay on station for days or even months on end, depending on their source of power, relaying back vital information about the adversary's force levels, deployments, communication traffic, electronic and underwater signatures, hydrological conditions, etc.

Increasingly, intelligence is also likely to be gleaned through cyberspace

and mobile networks. Today, the Internet has become all pervasive in our daily lives. The introduction of the smartphone in 2007 as well as the growth of social media networks have resulted in an enormous amount of communication and data being exchanged on the Internet on a daily basis. While the bulk of this traffic would be inconsequential, there could be some which may be of immense value to intelligence agencies. It would be impossible for human operators by themselves to listen to, process, analyse and disseminate useful intelligence – akin to finding a needle in a haystack the size of the entire world! However, new generation quantum computers when programmed with the right algorithms and keywords could doubtless do so in a very short time[51].

While a nation would like to collect as much intelligence on a potential adversary as much as possible, it is obvious that the target nation would try and deny this information. Hence, the need for an effective counter intelligence organisation. This is a vast subject which requires an entire paper by itself. Suffice it to say that all major powers have an equally effective counter intelligence organisation in their Govt.

Earlier, I described the requirement of intelligence for assessing the enemy's capabilities and intentions. While most of the foregoing discussion has been about capabilities, it is not so easy to gauge intentions – at least with regard to a conventional threat – even with all the technology available today. This year too, Ukraine was caught by surprise when Russia actually invaded its territory, despite all the signs of troop movements amassing along the border[52]. Speculation about if and when China will actually invade Taiwan remains just that - speculation, despite all the hostile military manoeuvres that Chinese forces have conducted off the island in recent months.

In the past, intelligence agencies have also been used not just to get more information about the adversary, but also to create a narrative and consequently try andinfluence decisions and actions. The British, for example, planted a number of stories about German submarines operating off the US coast in an attempt to bring the latter into the war[53]. And who can forget General Colin Powell's presentation to the UN, citing Iraqi WMDs, which led to the US invading that country for the second time (and deposing Saddam Hussein)[54]. Today, social media is a powerful medium that could be exploited by belligerent nations by planting fake news, which become viral and haveserious consequences.

The nature of warfare is constantly changing and with it the strategy and tactics employed by belligerent nations. We have already come a long way from the days when soldiers fought with swords, shields and spears, to the guns, tanks, battleships and carriers of the 20th Century. In the 21st Century, we are in an

era where hand to hand fighting may become increasingly uncommon. Rather, a belligerent would try and target an adversary using the latest technological systems and weaponry at his disposal, including through cyberspace. On the battlefield, this may well translate to Unmanned Autonomous Vehicles/Vessels using Artificial Intelligence to carry out missions without any human intervention. The belligerent would also use a host of sophisticated intelligence collection systems to obtain as much information about the adversary's capabilities, force structure and deployment pattern.

Indian Intelligence Organisation - Way Ahead

What does this mean for India and especially for its military? The saying "Change is the only constant" is quite well worn by now, but impossible to ignore. As with all other organs of our national security matrix, Indian intelligence agencies – primarily the R&AW, NTRO and military intelligence – have to adapt and develop their organisation, methods and intelligence assets to be comparable with those of our main adversaries.

There has been much change in the intelligence organisation and methodology in India, especially following the Kargil Review Committee Report. The setting up of the DIA and the NTRO are just two of the spinoffs[55]. However, an assessment of how good India's overall capability is today remains a grey area, considering the official cloak of secrecy that covers anything to do with intelligence. Still, if one were to go by the few documents have been published in the open domain, both by our own MPIDSA[56] as well as the UK based IISS[57], there is still a felt need for an objective audit of these capabilities to see where we match up with our main adversaries and if further reforms are necessary.

Some of these capabilities would include:-

- A comprehensive constellation of spy satellites – optical, radar and ELINT; including those for maritime surveillance
- Near real time monitoring of our adversary's communications (radio/ landline/ mobile/social media) using an automated, high speed crytologic system based on supercomputers and – in due course – on quantum computers with suitable algorithms and keywords to flag conversations of interest for further analysis.
- Development of AI based Unmanned Autonomous Vehicles/Vessels for intelligence collection.

- Sharing of information between various intelligence agencies, through an information grid using a distributed network. This must have a 'push-pull' type of information architecture, where one organisation – say Military Intelligence –'pushes'the information on to the network, which is then determined by Naval Intelligenceas relevant to its domain (based on a set of algorithms/keywords), and 'pulled' for disseminating to lower formations.
- Ensuring a high degree of professionalism and training of intelligence personnel (analysts) and attaches, and increasing their proficiency in foreign languages. A large percent of analysts should be 'vertically specialised' on the country of interest and have long years of continuity at their desk.

As with most cutting-edge technologies, intelligence collection and analysis systems can rarely be bought off the shelf, but have to be developed indigenously. Given that India has a large body of IT professionals and some of the smartest people in the world, there is no reason why we cannot do so. Without these systems in our inventory, those adversarieswho do possess them would get a head start in a future conflict. Most of all, the importance of intelligence needs to be given a high priority both by the political leadership as well as military commanders. Accomplishments of those who deliver results need to be rewarded and recognised– even if it is in private – so that we can produce our own Station Hypo and Ultra rather than be caught out by intelligence failures such as those at Kargil in 1999, Mumbai in 2008 and Pulwama in 2019.

References

1) *FM 2-0 Field Manual. US Army, 17 May 2004. p. 1-30*

2) *Ibid pp. 1-31 - 1-32*

3) *Smith, W. D. (1986, February 6). The Ideological Origins of Nazi Imperialism (1st ed.). Oxford University Press. p 4*

4) *United States Holocaust Memorial Museum, Washington, DC. (2021, August 20). German-Soviet Pact. Holocaust Encyclopaedia. https://encyclopedia.ushmm.org/content/en/article/german-soviet-pact*

5) *Hastings, M. (2015). The Secret War: Spies, Codes and Guerrillas 1939–1945. Macmillan Publishers.pp.14, 57-60*

6) *Hastings, M.The Secret War. Op cit: pp 152-153.*

7) *Ibid. pp. 66, 139*

8) *Hastings, M. (2022). All Hell Let Loose: The World at War 1939-45 (10th ed.). HarperCollins Publishers. p. 178*

9) *Ibid. p. 223*

10) *Hastings, The Secret War:loc cit p. p. 204*

11) *Holmes, W. J. (2012, October 20). Double Edged Secrets: U.S. Naval Intelligence Operations in the Pacific (Bluejacket Books). Naval Institute Press. p.64*

12) *Hastings, The Secret War loc cit. p. 212*

13) *US National Archives. (n.d.). Pearl Harbor: Why Was the Attack a Surprise? Google Arts and Culture. https://artsandculture.google.com/story/pearl-harbor-why-was-the-attack-a-surprise-u-s-national-archives/5QVRxdyVqxIA8A?hl=en*

14) *Ibid*

15) *Stile, M. (2011, November 22). Tora! Tora! Tora! - Pearl Harbor 1941. Osprey Publishing. pp 34-35*

16) *Stile. Op cit. p 217-219*

17) *Hastings, The Secret War, op cit. p 101*

18) *Ibid. p. 113*

19) *Ibid. p 510*

20) *FM 2-0 op cit. p. 1-30*

21) *China Military Power : Modernizing a Force to Fight and Win. (2019). Defense Intelligence Agency. https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf*

22) *The Central Intelligence Agency: An Encyclopaedia of Covert Ops, Intelligence Gathering, and Spies. (2016). ABC-CLIO, LLC p. 348*

23) *Ibid. p 281*

24) *Ibid. p 36*

25) *Sirrs, O. L. (2017). Pakistan's Inter-Services Intelligence Directorate: Covert Action and Internal Operations. Routledge p. 2*

26) *Ibid. p. 225*

27) *Ibid. p 280*

28) *National Security Agency/Central Security Service. (n.d.). About. Retrieved September 26, 2022, from https://www.nsa.gov/about/mission/*

29) *CIA Encyclopaedia. p. 339*

30) *Stokes, M. A., Lin, J., & Hsiao, L. R. (2011, November 11). The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. Project 2049 Institute. P. 5*

31) *Stokes, op cit.*

32) *Bajoria, J. (2008, Nov 7). RAW: India's External Intelligence Agency. CFR. Retrieved Sept 29, 2022, from https://www.cfr.org/backgrounder/raw-indias-external-intelligence-agency*

33) *https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf p. 43*

34) *Cyber Capabilities and National Power: A Net Assessment. (2021, June 28). In IISS. IISS. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power. p 134*

35) *Burrough, B., Ellison, S., & Andrews, S. (2014, April 23). Snowden Speaks: A Vanity Fair Special Report. Vanity Fair. https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview*

36) *CIA Encyclopaedia.loc cit.*

37) *CIA Encyclopaedia.op cit. p 118*

38) *Ibid p. 280*

39) *Ibid. p. 85*

40) *Norris, P. (2007, November 26). Spies in the Sky: Surveillance Satellites in War and Peace (Springer Praxis Books) (2008th ed.). Praxis.p. 22-27*

41) *Handbook of Satellite Applications (2013th ed.). (2022, September 27). Springer Verlag. P 117*

42) *Weeden, B. (2014, March 7). Through a Glass, Darkly : Chinese, American, and Russian Anti-satellite Testing in Space. SWF Issue Brief.*

43) *Ibid p.20*

44) *Kralina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology (Springer), p. 24*

45) *Murphy, J. (n.d.). John Murphys - Cold War Warriors: Spy Ships, Theirs and Ours. Emmitsburg.Net. Retrieved September 27, 2016, from http://www.emmitsburg.net/archive_list/articles/misc/cww/2011/spy_ships.htm*

46) *Kim, B. (1988, September 6). Moscow's South Pacific Fishing Fleet Is Much More Than It Seems. The Heritage Foundation. Retrieved September 27, 2022, from http://www.heritage.org/Research/RussiaandEurasia/asb80.cfm*

47) *Kannan, S. (2021, January 23). Exclusive: As Chinese survey ships map Indian Ocean, experts raise defence alarm. India Today. Retrieved September 27, 2022, from https://www.indiatoday.in/india/story/exclusive-as-chinese-survey-ships-map-indian-ocean-experts-raise-defence-alarm-1761945-2021-01-23*

48) *China's Military Power, op cit. p.79*

49) *"The Killing of Osama: Easy Operation as a Result of Hard Intelligence". Royal United Services Institute.", 6 May 2011, https://rusi.org/explore-our-research/publications/commentary/killing-osama-easy-operation-result-hard-intelligence.*

50) *Joint Military Attaché School Brochure, Defense Intelligence Agency, Feb 2022*

51) *Kralina, op cit, p. 8.*

52) *Kaplan, L. (2022b, May 12). Intelligence and the War in Ukraine: Part 1. War on the Rocks. Retrieved September 27, 2022, https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/*

53) *Ignatius, D. (1989, September 17). How Churchill's agents secretly manipulated the U.S. before Pearl Harbor. The Washington Post. https://www.washingtonpost.com/archive/opinions/1989/09/17/how-churchills-agents-secretly-manipulated-the-us-before-pearl-harbor/0881f7a8-7c9d-*

49d0-8338-eac3be333134/

54) *Powell, C. (2003, February 5). Remarks to the United Nations Security Council - Secretary Colin L. Powell. US Department of State. https://2001-2009.state.gov/secretary/former/powell/remarks/2003/17300.htm*

55) *V Dalmia, V Kapoor, & S Datta. (2020 Dec 9). India's Enduring Challenge of Intelligence Reforms. In ORF Online. Observer Research Foundation. https://www.orfonline.org/research/indias-enduring-challenge-of-intelligence-reforms*

56) *A Case for Intelligence Reforms in India. (ca. 2012). Manohar ParrikarInstitute for Defence Studies and Analyses. https://www.idsa.in/book/ACaseforIntelligenceReformsinIndia*

57) *Cyber Capabilities and National Power: A Net Assessment. (2021, June 28). IISS. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power*

ABOUT THE AUTHOR

REAR ADM
RJ NADKARNI
(RETD)

Rear Adm RJ Nadkarni (Retd) was commissioned on 01 Jul 1983, He is an ND specialist and a graduate of DSSC, CNW and NDC. During his career of more than 37 years, he held important command, training and staff appointments including three years as Director or Naval Intelligence (Operations) at Naval Headquarters. Post retirement he has settled down in Pune, where he is an active member of the CASS and IMF.

CENTRE FOR ADVANCED STRATEGIC STUDIES

The Centre for Advanced Strategic Studies (CASS), Pune was registered on 21st September 1992 under the Society's Registration Act, 1860, and as a Charitable Public Trust on 28th October 1992, under the Bombay Charitable Public Trust Act of 1950.

The Department of Scientific and Industrial Research, Ministry of Science and Technology, Government of India has accorded recognition to the Centre as a Scientific and Industrial Research Institution. The Centre has also been granted exemption U/S 80G of the Income Tax Act, 1961, which gives fifty percent exemption to the donors.

The Centre aims at undertaking research and analysis of subjects relating to national and international security and development through seminars, discussions, publications at periodical intervals and close interaction with the faculty members and research students in allied disciplines in the Universities and Educational Institutions as well as the Armed Forces.

In the coming future, the Centre expects to award research fellowships for studies in various areas of National Security and National Development. It aims to generate and promote interest among the academicians and public in related subjects, with a view to increase awareness to national security concerns. It has received very valuable support from the University of Pune in all its activities, especially from the Department of Defence and Strategic Studies. It has a Memorandum of Understanding (MOU) with Yashwantrao Chavan Academy of Development Administration (YASHADA), Pune for enabling mutual collaboration in the academic activities.

The Centre has held a number of seminars, panel and group discussions in the past. The Centre has also embarked on publishing a Quarterly Journal with effect from January 2014.

ADDRESS: Centre for Advanced Strategic Studies M.M.D.W. Potdar Complex, Savitribai Phule Pune University Campus, Pune – 411 007
Telefax No.: 020-25697516
Email: cfass1992@gmail.com Website: www.casspune.org

Centre for Advanced Strategic Studies (CASS)

Journal

---

www.casspune.org