
BHONSALA MILITARY COLLEGE
NASHIK
DAKSH
Vol No.:16
August 15th 2019
स्वतंत्रता दिन, रक्षाबंधन
श्रावण पौर्णिमा,शके १९४१

Dedicated to the Fond Memory of

Late Dharmaveer Dr. B. S. Moonje

The founder of

Central Hindu Military Education Society

Central Hindu Military Education Society

Central Hindu Military Education Society: A body devoted to promoting education

Dr. B. S. Moonje founded the Central Hindu Military Education Society, our parent body, in the year 1935. He was fired by the desire of Indianisation of the armed forces. He was a firm believer in the adage ‘MIGHT IS RIGHT’. He knew that the right path to independence of India was by empowering its youth in mind and body. Thus came into being the Bhonsala Military School, in the year 1937.

The society has a long tradition of past students who joined the Armed Forces, or have rendered commendable service to the society in such diverse fields as politics, civil services, and social service. The society has been fortunate in having at the helm such pioneers as Late Shri Bhavanishankar Niyogi and Late Gen. G.G. Bewoor (Retd.).

After independence, a new objective was added to the existing ones. It was now imperative to preserve the hard-earned independence; to uphold the integrity and sovereignty of India. Men and women were to be encouraged to actively participate in the armed forces and civil services. Together with Bhonsala Military School, we also offer preparatory military training to enrolled participants. Our motto is ‘a sound mind in a strong body’. We have slowly and steadily evolved a formidable system, which in the days to come will be a leader for institutions which offer military training, like IMA, Dehradun, and NDA, Pune.

Bhonsala Military College

Bhonsala Military College is a pioneer educational institution devoted to promoting military education. In the year 1986, the Bhonsala Military College came into existence. It is privately supported and partially residential co-educational institute. The primary objective of the institute is to provide for, and otherwise promote, education and research in the fields of Science, Humanities, Commerce, and Defence and Strategic Studies.

Vision

Bhonsala Military College is a pioneering institution which promotes academics with a perfect blend of military values in a caring, value based environment, which encourages students to be energetic, purposeful, creative, service oriented, responsible, dignified and integrated citizens to make a notable contribution to the armed forces and civil services.

Mission

With learning as its central mission, Bhonsala Military College responds to the needs of diverse students' community by offering high quality, affordable, and accessible learning opportunities for all round development of mental, physical and spiritual faculties through inculcation of strong value system culminating into national development.

Objectives

- ➔ To prepare students for the relevant University examinations
- ➔ To develop their personality by intellectual and physical activities
- ➔ To encourage students to take up careers in the Armed Forces of the country
- ➔ To prepare students for different competitive examinations conducted by M.P.S.C. and U.P.S.C.

Bhonsala Research Centre for Conflict & Peace

Bhonsala Military College is affiliated to the Savitribai Phule Pune University. The college is one of the few institutions in the country conducting courses in Defence and Strategic Studies up to the post graduation level. As an extension to Post Graduate Department, a research centre has also been opened under the banner, “Bhonsala Research Centre for Conflict and Peace”.

Objective

The main objective of this centre is to promote consciousness about National Security and identify solutions to conflicting issues at National and International Level.

Activities

The Centre conducts various activities such as Guest Lecture, Seminars, and Symposia. In addition, a quarterly publication named “Daksh” is a regular feature covering the research articles on a wide range of issues on National, Regional and International Security and Strategic affairs.

Daksh

Daksh is Quarterly publication of Bhonsala Research Centre for Conflict and Peace. It is the extension of other academic activities taken up by the post-graduate department of Bhonsala Military College based on the ideal Concept of the late Dharmaveer Dr. B. S. Moonje, founder of the Central Hindu Military Education Society.

To translate the noble ideas of Dr. B. S. Moonje into practice, in the light of contemporary security environments in large perspective, Daksh aims at projecting and analysing issues pertaining to security, and other related issues in the national, regional and global arena, and evaluate through interdisciplinary angles.

Each issue would feature idea, perception and thought from the scholars of various backgrounds on problems-past and present.

Instructions for Contributors

Original articles are invited in two double-spaced electronic copies (one PDF and one word file) of article/paper not exceeding 3000 words. The articles must be typed in Times New Roman with Font Size 12. The figures, graphs, charts, tables and other info-graphic representation should be numbered and must be in jpeg form. The paper must contain an abstract, keywords with proper reference/ footnotes at the end of the article/ paper. The paper must be accompanied with a brief Personal Bio-Data of the author. The paper should be mailed to the following email address: daksh@bmc.bhonsala.in. It is the sole responsibility of the author(s) to ensure the originality of the research paper. The Editorial committee or institution will not be held responsible for any consequences arising from plagiarism. Editorial committee reserves all the rights to accept or decline the submitted research paper. Authors should also ensure that the articles have not been published elsewhere prior to submission for Daksh. Reproduction of article/ paper in any form for other publication can be made with prior permission from the Principal, Bhonsala Military College, Rambhoomi, Dr. Moonje Path, Nashik-422005.

Disclaimer

Opinions expressed in the article are the sole responsibility of the author(s) and the advisory/editorial committee shall not be responsible for it.

Advisory Committee

Lt. Gen. Dattatray B. Shekatkar, PVSM, AVSM, VSM (Retd.)
President,
Governing Council
Central Hindu Military Education Society

Shri. Pramod G. Kulkarni
Working President,
Governing Council
Central Hindu Military Education Society

Dr. Dilip G. Belgonkar
General Secretary,
Governing Council
Central Hindu Military Education Society

Shri. Hemant P. Deshpande **:- Prabandhak**
Secretary
Nashik Division
Central Hindu Military Education Society

Editorial Committee

Shri.Vinay D. Chati **:- Managing Editor**
Head,
Department of Mass Communication & Journalism
Abasaheb Garware College, Karve Road, Pune

Dr. U. Y. Kulkarni **:- Co-ordinator**
Principal (A),
Bhonsala Military College,
Rambhoomi, Dr.Moonje Path, Nashik-05

Dr. P. A. Ghosh **:- Chief Editor**
Head & Associate Professor
Defence & Strategic Studies
Bhonsala Military College,
Rambhoomi, Dr.Moonje Path, Nashik-05

Shri. Mohit S. Purohit **:- Member**
Researcher,Kanhoji Angre Maritime Research Institute
Bhonsala Military College,
Rambhoomi, Dr.Moonje Path, Nashik-05

Articles Published in Previous Issues

Author	Title
Dr. L. Randeep Singh	Executive Editor's Note
Dr. Rajvir Singh	Changing Trends of Threat Perception and Internal Security Problems of India
Dr. L. Randeep Singh	Terrorism and Insurgency
Dr. Lakshmi Kumar & Dr. Govind Das	Uttarakhand : Creation and Repercussions
Lt. Gen. Ashok Joshi PVSM, AVSM (Retd.)	Apropos of CTBT
Dr. K. S. Sidhu	India's Nuclear Policy Retrospect and Project
Dr. Shrikant Parajape	SAARC, SAPTA and Politics of Economic Integration in South Asia
Big. A. A. Wagh (Retd.)	Policy on Science and Technology for National Development and Security
Maj. Gen. V. K. Madhok AVAM VSM (Retd.)	Military Technology Trap: Can India Escape Technological Colonisation?
Mr. L. A. Khan	Central Asia in Transition
Dr. Shrikant Paranjpe	US Attempt at Order in South-East Asia: SEATO Years.
Maj. Gen. K. S. Pendse (Retd.)	Synopsis of a talk on Global spread of Military Technology
Prof. (Dr.) P. M. Kamat	Nuclear Options
Dr. P. A. Ghosh	Achievements of IPKF in Sri Lanka
Dr. Lakshmi Kumar & Dr. Govind Das	Military Culture of Garhwal: Evolution and Impact on Society
Dr. Shrikant Paranjpe	U.S. Attempt at order in South-East Asia: SETo Years
Dr. Ch. Budhi	India's Integration Problem in the North-East and Social Sciences

Padmashri Dr. M. Kirti Singh	Youth's Mental unrest in Manipur
Dr. J. A. Khan	Trends and Compulsion of Going Nuclear
Dr. Lakshmi Kumar	Pakistan Missiles and security of India
Dr. V. Yoga Jyotsna	Threats to India's security : Significance of the Domestic Dimension
Maj. Gen. K. S. Pendse (Retd.)	Role of Science and Technology 159 in India's Resurgence
Dr. Sanjay Deshpande	Regional Politics in South Asia
Dr. Nand Kishor Kumar	India's Armed Forces and Gandhi
Dr. L. Randeep Singh	Concepts and Parameters of India's National Securities : A Short Assessment
Dr. P. M. Kamath	India's Nuclear Strategy : The Post-Pokhran Phase
Brig. K. G. Pitre AVSM (Retd.)	New Atomic Balance of Power in South East Asia
Mr. Vikrant J Kawale	Internal Turbulence and Development of Army
Wg. Cdr. S. M. Shukla (Retd)	On Happenings in "Kargil"
Dr. Lakshmi Kumar Mishra	Pakistan's Taliban Hand Endangering India's National Security
Dr. M. L. Sali	Border Dispute Among Nations : A Holistic View
Mr. Vijay Khare	India's National Security Council Perception, Practice and Prospects
Lt. Col. Rajiv Kapoor	International Target Acquisition Through Satellite –Readers
Maj. Dipak K Das	Indo-Us Relation and Policy Option in Next Millennium
Dr. W. N. Bhende	India's Nuclear Policy in Nut-Shell
Lt. Col. Rajiv Kapoor	Need Metamorphose The Indian Army
Mr. Vijay Khare	Social Mobilization and India's National Securities Problems and Prospects

Dr. Agha Mansoor Khan	Chemical & Biological Warfare
H. Nilamani Singh (Ex.I.N.A.)	I.N.A. Headquarters, Moirang-1944
Late Col. P. K. Sahgal (Ex.I.N.A.)	Victory in Defeat
Dr. P. A. Ghosh	Multi-faced Aspect of Internal Security : India
Mr. Nilesh Saudagar	Psychological Aspects responsible for corruption : India
Dr. J. A. Khan	Human Right and Security Forces
Dr. A. R. Bharadwaj	Some Aspects Related to Military Psychology
Dr. V. V. Raje & Mr. S. D. Joshi	Human Rights & New Economic Policy- Indian Context
Mr. Vijay Khare	Sri Lankan Ethnic Crisis and Strategic Implications to India's National Securities
Lt. Gen. D. B. Shekatkar AVSM, VSM (Retd.)	Counter Insurgency & Human Right
Lt. Gen. A. S. Parmar PVSM ADC (Retd.)	Human Right
Gpt. Cpt. S. G. Chitnis AVSM (Retd.)	Low Intensity Conflict: Counter Insurgency and Human Right
Maj. Gen. B. N. Rao AVSM, VSM & Bar (Retd.)	A Military Centric View of Human Rights in Counter Insurgency Operations
Prin. S. B. Pandit	Human Right Challenged by Terrorism
Arunkumar Bhatt	Human Right : Weapon of Psychological Warfare in Insurgency
Dr. J. P. Palande	Human Right and the Constitution of India
Mr. Vijay Khare	Human Right in India : Issue and Perspective A Case Study of Child Labour
Dr. Shrikant Paranjpe	Self-determination, Session and the Human Right Debate in India
Lt. Col. S. K. Khasgiwale (Retd.)	Media Relation in LIC Environment
Dr. Dilip Ukey	Human Right in India A Constitutional Imperative and Judicial Creativity

Dr. S. R. Chakravarty	Pakistan: Problem and Prospects of State Building
Dr. Nand Kishor	Cross Border Terrorism in Kashmir
Dr. A. S. Dalvi	Future of Nation State System
Dr. Shrikant Paranjpe	Implication of American Counter Terrorism Strategy
Mrs. M. A. Bharadwaj	Trauma After War
Mr. Vijay Khare	Non-Military Challenges to India's Security
Dr. Amit Dholkia	How Dare You!
Prof. P. L. Dash	Chechnya : War Has No End
Lionel Fernandes	The United Nation and A New World Order
Dr. M. L. Sali	A Study of Bodo – Land Movement
Prof. Phadke U.S.	The Importance of Island Security
Dr. P. A. Ghosh	Ethnic Conflict and Security Crises in India : A Case Study of Tribal Insurgency in Tripura
Dr. J. A. Khan	Development Trends in Defence Material
Dr. Debabrata Goswami	International Security and Countering Terrorism: A Brief Account
T. Chakraborti	Insurgency in Tripura and India's Security
Vikas Kumar Singh	Science, Technology & Security
विनीत सिंह	विज्ञान तकनिकी : भारतीय सुरक्षा के बदलते आयाम
Dr. V. P. Nedunchezhiyan	The Importance of Island Security
Dr. Nand Kishor	The Challenges of Nuclear Technology
Mr. Vijay Khare	India's defence Policy: An overview
Mrs. M. A. Bharadwaj	War Neurosis

From the Desk of Chief Editor

It is a known fact that education helps in developing inner strength of the mind. Moreover, it helps an individual to build self-confidence, focused attitude and his own potentialities. May be for this reason, Swami Vivekananda had described education as, 'the man making process' and that helps in developing character of the individual." A good and positive character can help in spreading positivity around him. He helps an individual to become a good human being. Such a being will be free from ego, down to earth and always ready to help others who are desperate. He may help to develop goodwill among individuals that ultimately lead to the unity of compassion. The sage had also reiterated that education transforms an individual to be a flexible entity to form the attitude of self- sacrifice, humbleness, and selfless work for others with full dedication without pride, ego and negative attitudes. Further, quality education leads towards the attitude of a person to resolve societal and his own problems. A self-sufficient individual certainly will develop an attitude of love for learning and acquisition of knowledge from the nature. Hence, an individual strives to be equipped with the advancement of knowledge, skills and technology that is relevant to him and society at large. Besides this, there is no substitute for quality in higher education, although the country has been facing a serious problem of meeting the needs of our society for a long time. It is, therefore, essential that a careful balancing of the two be given priority to meet the twin requirements of the society.

As we are aware, most of the third world countries and its people face many challenges, crises and forces of division — such as poverty, violence, and human rights abuses — among many others — which undermine peace, security, development and social harmony among the people. Hence, Challenges to human life are enormous and they cannot be solved by governments alone unless people understand the genesis of such crisis and find out best methodology towards conflict management and resolution aimed at, to create a better environment to live in. Moreover, every individual must have adequate sense of security in their minds and justice and equality must prevail that ensures the basic necessities of life. Thus, it involves the elimination of violence, oppression, greed and environmental destruction by the constructive mediation of conflicts. Hence, there is an urgent need to create awareness amongst every citizen of the country to understand the causes of conflict and thereby find answer to the question how violence can be prevented and peace can be established throughout the society, which is indispensable towards development of the state.

In an effort to create human resources and expertise as well as school of thought to contribute towards strategic thinking in the field of defence and strategic studies, the C.H.M.E

Society Officials and Principal of the college decided to publish 16th issue of 'DAKSH', a half yearly Security Studies Journal under the roof of Bhonsala Research Center of Conflict and Peace (B.R.C.C.P)., an independent branch of Defence and Strategic Studies Department. Against this backdrop, it is my privilege to express my sincere thanks to all the Society Officials and Principal of the college, for their constant support, guidance and encouragement towards publication of this issue. Without their support and encouragement it would have not been possible to publish the current issue in time. The journal named 'DAKSH' is multi disciplinary in approach which is aimed at objective analyses on a host of subjects related to India's and International Security Management studies that form the core of strategy in different areas. Filling the existing vacuum on the subject, the collection provides access to matured thoughts with a strong and convincing narrative. I am sure, the journal would appeal to a wide cross section of the scholars and students' fraternity and those interested in India's national security studies and International Affairs.

Dr. Priyanath A Ghosh
Head, Defence and Strategic Studies Department
Bhonsala Military College

Index

Technologies and Camouflage Warfare

Dr. Priyanath Adinath Ghosh
Head, Defence and Strategic Studies Department
Bhonsala Military College, Rambhoomi, Nashik-05
M.Phil & Ph.D. Research Guide, Savitribai Phule Pune University
Email: drpaghosh@gmail.com

Introduction:

The concept of national Security was understood differently by various experts on various occasions ranging from the "the ability of a nation to protect its internal values from the external threats" to "the preservation of its core values critical to the nation- state from external and internal threats". A state is deemed to be secure when it does not have to sacrifice its national interests to avoid war and is able to maintain by waging war, if required. The notion of security has spanned from territorial integrity through national interests and the political, economic and social well-being of the government policy that aims to create national interests against existing or economic, political, military and social threats". National security thus "comprises every action by which a society seeks to assure its survival and realizes its aspiration internationally." It can be mentioned that in the 21st century, the forces we have to fight are dynamic and challenges are new. Threats from internal and external are unpredictable and therefore we cannot conceptualize war doctrine ignoring the recent trends of the dynamics of the society. Because, the last two decades have brought into sharp focus an alarming and at times disastrous processes in the relationship between man and man and countries. Newly independent and developing countries where people's behavior is passing through a transitional phase under different socio-political and eco-ethnic compulsions and thrust of modernizations continuously increasing with age old tradition, contains in itself different problems of the present time. New trends in security environment require wide-ranging review for clear understanding of people security problem worldwide.[1]

Comprehensive human security is concerned with the problems of everyday life. It is not only concerned with weapons; rather it is concerned with the condition of human life and feelings in terms of individual safety and security. The legitimate concern of the ordinary people is to ensure security in their daily lives. For many, security symbolizes protection from any kind of threats like diseases, crime, social conflict, political repression, environmental hazards, displacement etc. Hence, Security consists not only of military aspects, but also political, economic, social, human rights and ecological aspects. Under development and declining prospects for development, as well as mismanagement of resources, constitute challenges to security. The security of individuals and

communities of which states are constituted is ensured by the guarantee and effective exercise of individual freedom, political, social and economic rights as well as by the preservation or restoration of inhabitable environment for present and future generations. Moreover security also implies that essential human needs, in the field of nutrition, education, housing and public health are ensured on a permanent basis.[2] Therefore, the way and means to attain security may be defined in national, intergovernmental, non- governmental, regional or global terms. A nation has security when its people don't have to compromise to their value of life and have feelings of security, and thus states do not have any threat of military aggression, political pressure or economic oppression etc. Thus, states are able to pursue freely their own developmental activities and progress. Security has an extended meaning beyond its obvious military connotation; there is better appreciation now of its non-military and human dimensions. Hence, the state needs to cater for its own and its individual's security. Thus, the imperative necessity is to have good governance to achieve the ends of both state and individual security.[3]

Technologies and National Security

Technology is a great source of national power. Having understood the role of technology in power politics, all developed nations engaged themselves to have access to superior technology. Former Soviet-Union, United States of America, Germany, Japan are developed states due to their superior technology. They always keep a watch on the development of all over the world and make sure that they do not fall behind vis-a-vis other nations particularly, in the field of weapon technology. Against such background, developed countries tremendously increased new technologies in every field and thus gained abilities to influence and control the behavior of less technologically developed nations in the world system. The impact of technology on warfare has always proved as a battle winning factor and thus evolution of war technology taking place along with that of mankind. Today, exploitation of high technology in developed countries has become one of the vital principles of war. Unlike third world countries, developed countries have understood that possessing obsolete technology is a disadvantage in terms of power status in international politics. Rapid changes in the evolution of new technology has not only affected the tactical environment of war but also entire strategic planning process of the country. Now technology alone governs the military capacity of a nation and thus has become a major factor in formulating a nation's strategic planning. Due to unprecedented advances in this field has reduced the role of geographical conditions. For example, in the air, no nation has geographical barrier along with its national frontiers to prevent the enemy and thus, air power forced all national policy makers

to reorient their strategic concepts in the domain of politico, economic and military life of the people.

The world has witnessed two significant events during the last three decades which has changed the contours of global strategic thought. The first being the end of the cold war and the second is the September 11, 2001 World Trade Center (WTC) terrorist attacks (9/11). The end of the cold war could be said to have started a phase of unilateralism with United states (U.S) being in the so called 'command of the world affairs; while the 9/11 attacks could be said to have challenged the hegemony of the U.S to such an extent that they are still unsure about how to address this asymmetric challenge posed by the terrorist organizations. So in a way it could be argued that the end of the cold war created opportunities for the US dominate while 9/11 could be said to be the US Achilles' heel.

During last few decades the whole world has witnessed an exponential growth of technology. This growth has not remained restricted to few limited fields but various new/applied fields have emerged leading to significant changes into lifestyles. From security perspectives impact of technologies has become an important premise of study particularly, in the area of information warfare. The impacts of science and technologies on international security environment are all encompassing. Technology is instrumental in influencing the concept of war-waging' in the minds of both the political and military leadership for many centuries but it appears that in the present scenario, it has almost become overarching. Modern day wars are not always envisaged to be fought only on the battleground. 21st century defence preparedness involves demonstration of technological strength dictated by the market forces. Hence, state and non-state actors are trying to gain superiority over the enemy by deploying qualitative software advanced technologies. The enhancing relative combat effectiveness is being achieved by integrating a number of evolving technologies. Developments of remote sensing, night vision, sensors, precision guided ammunitions, stealth technology and above all digital communications and computer networks are resulted new war fighting techniques. The current "silent" revolution in military affairs, however, has not been accompanied by an examination of its impact on force structures, organizational aspects, and doctrines, quality of leadership, human resource development and logistics. The 20th century saw the face of warfare being changed by mechanization, aviation and communication; the 21st century would see, with the help of evolving technologies, armed forces conducting knowledge-based warfare. In the Indian-subcontinent, future war will be a hybrid of the industrial age and knowledge based warfare. As Van Creveld says in his book Technology and War, *"the greatest victories that have been won in war do not depend upon a simple superiority of technology,*

but rather on a meshing of one side's advantages with the other's weakness so as to produce the greatest possible gap between the two." The Vietnam War was one such example. We, therefore, need to understand the technology driven changes and evolve doctrinal precepts to meet the challenges of warfare in the next century. Although technology is making great advances, human beings remain the most effective systems for determining relevance and fusing information. The Falkland and Gulf War clearly demonstrated that technological superiority has a pivotal role to accomplish a military mission. The complete suppression of Iraq's air led coalition forces, made it quite clear that developing countries need to review threat perception. Thus, it can be safely predicted that the future wars would continue to be fought with most sophisticated weapons that the technology of today would offer tomorrow. As we enter the information age, there is no doubt that information warfare technologies, precision fire technologies and fusion of a host of other technologies are going to transform the way we conduct warfare. Yet our intellectual thought processes need to be tempered by the limitations and possible vulnerabilities of these technologies.

Camouflage / Information Warfare

Various innovations in the recent past in information technology fields and communications have helped militaries to make their basic hardware and support infrastructure faster, secure and dependable. On the other hand, innovations in the fields like composite materials and nanotechnology have made the platform lighter and stealthier. Armed forces and states dependencies on various technologies for fighting war could be said to have brought in the concept of Revolution in Military Affairs (RMA). This involves induction of computer networks that confer information superiority, allows precision strikes on the targets, permits dominant maneuver, and undertake usage of space based assets for military purposes. Presently, RMA technologies are changing the nature of war-waging by enabling precise destruction of targets from a distance and speeding up the processes of decision making. The advent of RMA clearly indicates how technology plays an important role in regard to national security.

Two technologies that have dominated the entire landscape of military revolution particularly during the last two to three decades, are information technology (IT) and space technologies. The presence of both these technologies has been instrumental in bringing the concept of network centric warfare to reality. These technologies have succeeded in converting the modern day battle fields into digital battlefields. C4ISR capabilities and net-work centric tactics have become an important element of war fighting in the 21st century. Developed states and few developing states, have understood the relevance of technology from national security perspective

and therefore focusing in establishing information-based society and digitally stronger. This 'Information Revolution' is a product of advances in computerized information and telecommunications technologies and related innovations in management and organizational theory. Today, rapid and far reaching changes are occurring in how information is collected, stored, processed and disseminated, and in how organizations are designed to take advantage of this increased availability of information. The Information Revolution is setting in motion forces that challenge the design of many institutions. It disrupts the hierarchies around which modern institutions—traditionally have been designed. It diffuses and redistributes power, often to the benefit of those that once may have been considered lesser actors. These changes will inevitably have a profound impact on the means and ends of armed conflict. Due to the revolution in information and communication technology, the 21st century is known as the Age of information where citizen, businesses, military and the government are increasing relying upon information technology (popularly known as internet) for its delivery of services. Today information technology offers a wide range of services like E-banking, E- commerce, tele-medicines, online trading, mobile banking, payment gateways, public distribution systems, e- learning, virtual classroom, 24X7 surveillance, seeking public opinion on policy making and law enforcement etc. As we move on, reliance to the information technology will continue to increase. Along with this rapid rise, there would be an increased threat and vulnerability to the cyberspace i.e. from cyber crime; which would catastrophic in nature if the dangers of information and communication technology are not foreseen and planned. Sophisticated cyber criminals are increasing and exploiting cyberspace by stealing information, conduct financial forgery and to destroy critical infrastructure and to disrupt delivery of essential services. Thus, threats emerging from the cybercrime cannot be ignored; failure to do so, it would spoil the reputation in the international arena. Today, cyberspace is treated as the fifth domain of warfare along with land, sea, air and space. The United States of America has declared cyberspace to be the fifth domain of warfare and revised its military doctrine and hence has reserved the right to take all actions, including the right to take military action against nation states government has also formed strategic unit known as US Cyber Command in order to deal with such a scenario. Similarly, in 2010 the Republic of China overtly introduced its first department dedicated to defensive cyber warfare and information security.[4]

The information revolution erode the monopoly of information in the hands of governments; democratizing access to breaking information. Global networks provide transparency to everybody, making it difficult for countries unilaterally to take national policy decisions when the problems are global. Globalization and global networks also allow business firms to think and act in terms of

global production and global marketplace, heightening their international influence. Global network empowered and vastly increased the number of Non-Governmental organizations (NGOs) and even individuals on the international stage. NGOs now create, track and disseminate information and organize people and groups sympathetic to their goals to pursue specific policy outcomes in areas such as human and women's rights. The information technologies have had tremendous security, political, social and cultural consequences; altered roles of countries, companies, non-governmental organization (NGOs) and individuals. Global communications has enabled and empowered new nongovernmental institutions and accelerated and broadened transnational contacts between states and non-state actors in other countries. Global networks and new communication technologies have empowered non-state actors and democratized access to information. The consequences of global networks and communications are cut across border and issues. The results are both positive and disruptive, raising new opportunities and challenges for global stability. The information revolution altered the nature of intelligence operations, political and the waging of war. However, access to more information does not automatically translate into better policy decisions for greater national security.[5]

Every day, millions of people use the internet to search for different kinds of information stored in computers and databases that may be on the other side of town or half a world away. While most of these users access data legitimately, some use illicit ways to access and invade other computers. It is extremely hard to protect systems from all types of unauthorized access. Sophisticated hackers and crackers work diligently to find security loopholes and use these loopholes to break into systems. Besides attack from outsiders over the network, there remains the possibility of an invasion of one's system by an insider turned foe. Any such malicious attack against an organization's information base through electronics means is termed information warfare. Such an attack may be intended to cause temporary turmoil in the operations of the organizations including denial of service, or even to cause extensive damage to the organizational information. The public telephone network, banking and finance, vital human services and other critical infrastructures are dependent upon information technology for their day to day operations and must be adequately protected. In this context, IW means that actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information systems and in the process achieving an information advantage in the application of force. It is also an action to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending our information and information systems.[6]

New threats of the twenty-first century come from terrorists or any criminals who can exploit the technology and structure of the Internet. The term information warfare can mean the use of smart technology in a traditional war or the use of IT systems attacking a part of a country‘s infrastructure. The common fear appears to be the vulnerability of the latter. In some cases it appears the national laws cannot stem the tide of these emerging groups and governments are responding to this new threat with draconian measures by introducing electronic surveillance and interception to combat the increasing use of encryption favoured by terrorists and criminals alike. Governments have to strike a balance between freedom of speech on the other hand and the security of a country and its people on the other. Information warfare consists of both offensive and defensive components. Offensive information warfare seeks dominance over the enemy's information, computer information systems, and control systems using a myriad of tools. Attacks can be launched against the enemy's physical computer network, its supporting infrastructure, or a product of the network. The attacks can be overt or covert and consist of either hard or soft kills. Preemptive offensive information warfare may deter a potential enemy and offer coercive leverage to resolve crises in favour of lawbreaker. Effective covert offensive information warfare can reveal with near certainty, the operations of the enemy or disable their systems. Defensive information warfare seeks to preserve and protect its national information infrastructure by providing secure communication links and when required. Information warfare allows potential attackers to hide in the mesh of internet worked systems and often attackers can use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers anonymity and invalidates established "nation state" sanctuaries. Information warfare is also relatively cheap to wage, relatively simple and is extensively available worldwide. IW can be used to achieve national strategies. IW involves actions taken at the national strategic level to create an information gap between what is understood regarding the political, economic, cultural, and military strengths, vulnerabilities, and interdependencies of a potential adversary and what the adversary possesses regarding friendly capabilities.[7]

IW is has its own characteristics; (a) nation initiating the cyber attack is substantially lower than the risk for a party or nation initiating a traditional attack. This makes it easier for governments, as well as potentially terrorist or criminal organizations, to make these attacks more frequently than they could with traditional war; (b) information communication technologies (ICT) are so wrapped up in the modern world that a very wide range of technologies are at risk of a cyber attack. Specifically, civilian technologies can be targeted for cyber attacks and attacks can even potentially be launched through civilian computers or websites. As such, it is harder to enforce

control of civilian infrastructures than a physical space. Attempting to do so would also raise many ethical concerns about the right to privacy, making defending against such attacks even tougher; (c) integration of ICT makes it much harder to assess accountability for situations that may arise when using cyber/robotic attacks. For robotic weapons and automated systems, it's becoming increasingly hard to determine who is responsible for any particular event that happens. This issue is exacerbated in the case of cyber attacks, as sometimes it is virtually impossible to trace who initiated the attack in the first place. The innovation of advanced and autonomous ICTs has engendered a new revolution in military affairs, which encompasses nations' use of ICTs in both cyberspace and the physical battlefield to wage war against their adversaries. The three most prevalent revolutions in military affairs come in the form of cyber attacks, autonomous robots and communication management. Within the realm of cyberspace, there are two primary weapons: network centric warfare and C4ISR, which denotes integrated Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance. Furthermore, cyberspace attacks initiated by one nation against another nation have an underlying goal of gaining information superiority over the attacked party, which includes disrupting or denying the victimized party's ability to gather and distribute information. A real world Occurrence that illustrated the dangerous potential of cyber attacks transpired in 2007, when a strike from Israeli forces demolished a nuclear reactor in Syria that was being constructed via a collaborative effort between Syria and North Korea. Accompanied with the strike was a cyber attack on Syria's air defences, which left them blind to the attack on the nuclear reactor and, ultimately allowed for the attack to occur. An example of a more basic attack on a nation within cyberspace is a Distributed Denial of Service (DDOS) attack, which is utilized to hinder networks or websites until they lose their primary functionality.4 as implied, cyber attacks do not just affect the military party being attacked, but rather the whole population of the victimized nation. Since more aspects of daily life are being integrated into networks in cyberspace, civilian populations can potentially be negatively affected during wartime. For example, if a nation chose to attack another nation's power grid servers in a specific area to disrupt communications, civilians and businesses in that area would also have to deal with power outages, which could potentially lead to economic disruptions as well. Moreover, physical ICTs have also been implemented into the latest revolution in military affairs by deploying new, more autonomous robots (i.e. – unmanned drones) into the battlefield to carry out duties such as patrolling borders and attacking ground targets.[8]

Cyber warfare / crime

The use of a computer as an instrument to promote illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating privacy. Cybercrime, especially through the internet, has grown in importance as the computer has become central to commerce, entertainment, and government. Cyber crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information system, including any device or the internet or any one or more of them. Cybercrime can be defined as criminal activity done using the computer and the internet. This includes anything from stealing millions of rupees from an online bank account to creating and distributing viruses on the computer network or posing confidential data of the business and the government on the internet. Cyber crime mainly targets computer network or devices. These types of crimes include viruses and denial of service (DoS) attacks. Computers networks are also being used for the purpose of criminal activities like stalking, identity theft or carrying out terrorist attacks. Cybercrimes incorporate harassment to an individual through internet by sending e-mail and spam messages, trafficking, posting and dissemination of obscene material including pornography and indecent exposure. Cybercrimes are also committed against all forms of property; these crimes include computer vandalism (destruction of others' property), transmission of harmful programmes and viruses or controlling and damaging computer networks.[9] The cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests when an individual "cracks" into a secure government website or military maintained website and causes damage to critical infrastructure.

Smart Cities emerge from innovations in information technology and they create new economic and social opportunities. Humans are already connected via smart phones and gadgets; security devices are being used in many cities. Homes, cars, public venues and other social systems are now well connected through internet. Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life. To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation. Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery. Two important and entangled challenges are: security and privacy. Security includes illegal access to information and attacks causing physical disruptions in service availability. As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear.

Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand in hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live.[10]

Conclusion

In the context of international relations and diplomacy, power is normally considered as the ability of one state to influence or control other states. Technological revolution is essentially a dynamic process and is constantly evolving and its impact on society as a whole and national security in particular will vary with the process of scientific evolution and discoveries. The consequences of global networks and technical revolution is communications are both constructive and troublemaking, raising new opportunities and challenges for individual, national and international stability. As a result of networks, modern war is practically based on cyber platform where it has shown how cyber attackers use same old camouflage theory and techniques to apply in virtual battle ground i.e. internet and achieve target without getting captured or attacked. War in today's time after the involvement of Computer is not limited to direct, limited or total war; it has now become all time war and where citizens, businesses, military are made their target. Waging styles of war has changed due to evolution of time but its root remains same with basic principles being unchanged where for destabilizing a nation, its citizens are made target as targeting population compels the target nation to surrender because citizens by then rise in revolt against Government for failing to provide security. Cyber war surely going to be the field of all future wars where nations will develop more ways to integrate cyber into physical arena by inducting more weapons like laser or electromagnetic into its arsenal as strike weapon than nuclear weapons. The WiFi waves are used to download songs or videos and attackers are trying to install backdoor in system and will focus on damaging more physical resources and persons like that of increasing speed of CPU fan thereby causing huge harm to human life. Improvised techniques might also add in exploding of battery by manipulating codes or sometimes by generating a reflex action i.e. sending back the same amount of energy to the socket or main line causing chance of power shock to human or sometimes sending huge wavelength of sounds to human ears when headphones are connected making virtual contract killing quiet possible. Days are near when computer virus will not only limit itself to infecting systems but to go on for preying on humans who are operating it as this can be very well possible if genius brains(hackers) in cyber world comes with combinations of chains carried out in systematized channel.

Footnotes

Ghosh P.A, "Rational and Problems of Strategic Studies" in Conceptualizing Security for the 21st Century, Gautam Sen (ed), (Atlantic Publisher, New Delhi, 2007), PP.342-343

Ghosh P.A, "Ethnic Conflict in Sri-lanka and role of IPKF", (APH Publisher, New Delhi, 2000), PP. 2-3

Onkar Pawar, "Internal Security Problems in NER", (Kalpaz Publications, New Delhi,2016), PP.36-37

Guri, Yosef, Andrev, Yuval, Disk Filtration: Data Exfiltration from speakerless Air- Gapped, http:/arxiv.org/tp/arxiv/papers/1608.pdf

http//www.idsa.-india.org/an-apr9-9.html , www.jourals.savap.org.pk 2012

http://www.heritage.org/research/reports/2016/12/Cyber-attack-on-US-companies in 2016 Gokhle B.N, "Winning The War Without Weapons" in Defence and Security Alert,PP.18-19

http://cybercrime.org.Za/definition https://en.wipidia.org./wiki/information_ warfare 4/9out burned 2/27/2017

CLIMATE CHANGE:

Our greatest National Security THREAT?

Dr. Abhaya K. Singh
Associate professor,
Department of Defence & Strategic Studies,
K. S. Saket Post Graduate College,
(Dr. R. M. L. Avadh University),
Ayodhya,-224 123- Bharat
Email: draksraghuvanshi@gmail.com

It is not predicting the future that matters, but being prepared for it.

- Pericles, Greek statesman, 493–429 BC

Nature cannot be fooled.

- Richard P. Feynman

Introduction

Climate change is no more an environmental concern. It has emerged as the biggest developmental challenge for the planet. It is a grave threat to national security. While there are many national security challenges facing the nation, climate change is an aptly described "super wicked" problem that accelerates existing threats. It is also manifestly unjust. It is cruel irony; the poorest nations of the world that contributed the least to global warming will bear the brunt of climate change's impact. What we as a society, choose to do or not to do now will define the welfare of future generations. Their fate is increasingly shaped by climate change's dramatic, erratic and catastrophic national security.

The national security experts have begun to speak up louder and actively engage with the world's most authoritative climate science reports in their own threat assessments. The Office of the Director of National Intelligence (ODNI), Australia issued a clear-eyed threat assessment report that highlighted climate change's destabilizing effects. It stated that the "negative effects of environmental degradation and climate change will impact human security challenges, threaten public health, and lead to historic levels of human displacement." According to ODNI report, "global environmental and ecological degradation, as well as climate change, are likely to fuel competition for resources, economic distress, and social discontent through 2019 and beyond.

Climate hazards such as extreme weather, higher temperatures, droughts, floods, wildfires, storms, sea level rise, soil degradation, and acidifying oceans are intensifying, threatening infrastructure, health, and water and food security."[1]

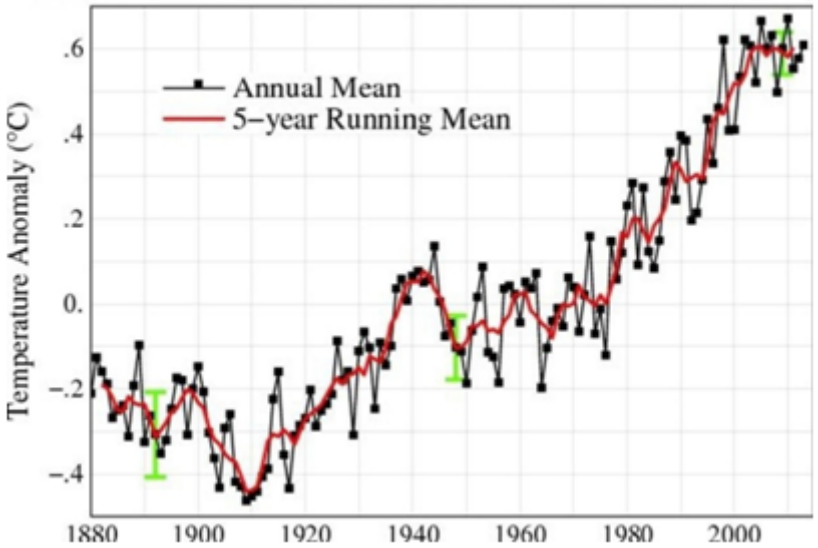
National Security and Climate Change

Perception of threat has been changing from time to time, but state was always the key actors in security. Some time it protected its people from external threat and some time it created threat to its own people. National security is about protecting the boundary from external actors. But, what should be done when the external actor is not one state or two states? How to recognize the enemy? How to solve the threat in the absence of clear enemy? These questions become relevant when we discuss the climate change? There is no one single actor which can be made responsible for the climate change. Climate change is a problem which will impact all the actors in international actors. It has the capacity to pose a threat to national security of a nation. This paper is an attempt to understand these questions in the light of climate change and Indian national security. The paper will also try to look in to the measures India has taken to reduce the impact of climate change on its national security at domestic level as well as international level and end with few suggestions for better mechanism to deal with climate change and its impact on national security.

The Center for Naval Analysis (CNA), USA report of April, 2007 on "National Security and the Threat of Climate Change" has clearly stated that 'when climates change significantly or environmental conditions deteriorate to the point that necessary resources are not available, societies can become stressed, sometimes to the point of collapse.'[2] The UN Security Council also identifying the impacts of climate change as a threat to international peace and security. Nothing can be more severe as a looming threat to humanity than the rapid climatic changes witnessed by the world today. The UN Security Council Secretary General, Ban-Ki-Moon said on 20th July, 2011 that 'possible adverse effects of climate change may, in the long run, aggravate certain existing threats to international peace and security'. The UN Secretary-General also said that climate change was an "unholy brew" that could create dangerous security vacuums, and that we must address a clear danger that not only exacerbated the threats but was itself a threat to international peace and security.[3]

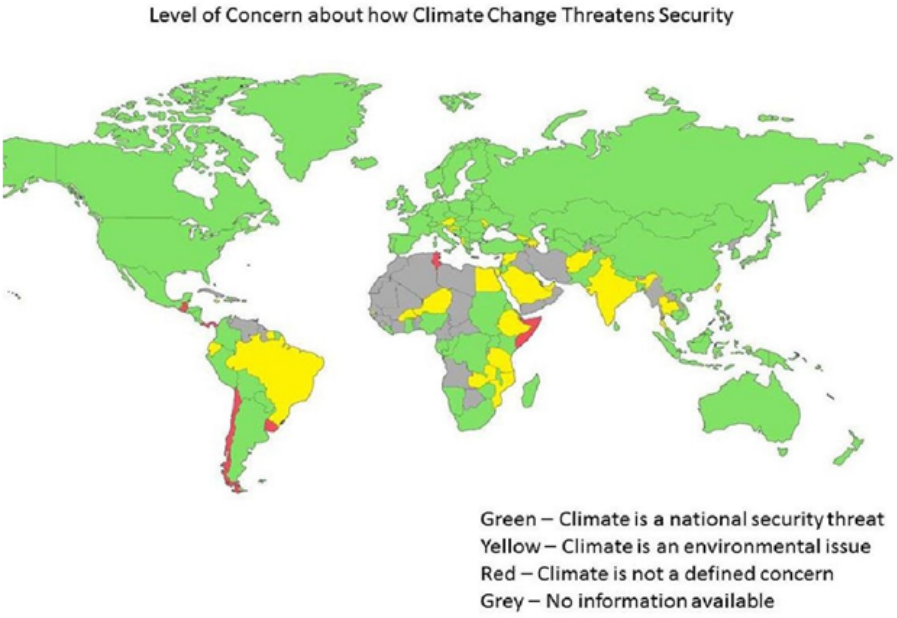
The impact of climate change on national security covers a wide spectrum. The recent scientific assessment presents a worrying picture. According to the Fourth Assessment Report of IPCC 2007, eleven of the last twelve years (1995-2006) rank among the twelve warmest years since 1850. The 2007 IPCC report predicts temperature rise of 1.1 - 6.4 °C by 2100. The number of

natural disasters in the world may double during the next 10 to 15 years. Over the past ten years, 3,852 disasters killed more than 780,000 people, affected more than two billion others and cost a minimum of $960 billion.[4]



(Changes in global surface temperatures since 1880)

Climate change is best viewed as a threat multiplier, which may create or exacerbate insecurities and tensions from the individual to the international level. Climate change does not simply mean the interaction between human beings and their environment. It implies a destabilizing interference in the ecosystem's equilibrium, which having negative implications on human society, expresses what is meant by environmental change of conflict. We adopt the Intergovernmental Panel on Climate Change's definition of climate change as a "change in the state of the climate that can be identified (e.g. by using statistical tests) by changes in the mean temperature and/or the variability of its properties and that persists for an extended period, typically decades or longer."[5] Additionally, climate change may be due to natural or manmade causes. At least 110 nations have identified climate change as a threat to national security.[6]



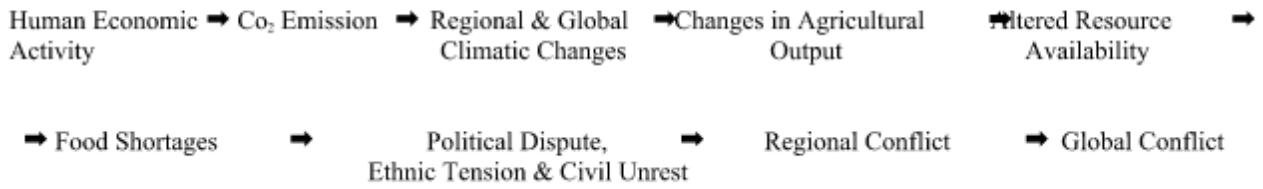
ASP's Global Security Defense Index on Climate Change, USA

The question arises how climate change leads to national security? The relationship between climate change and security is here to stay and it would be myopic on the part of the security establishment to not take cognizance. The political compulsions of public posturing should not deter the establishment towards combating the changing security scenario in their backyard. Failure to recognize the devastating implications of climate change on peace and security could prove to be very costly resulting in the worldwide instability and retarded development not to mention – loss of human life. In complex web of social, political, and economic causes and effects of conflicts, to explore exclusively the environmental causes of conflicts is undoubtedly a Herculean task. In the words "climate change may contribute to conflicts as diverse as war, terrorism, or diplomatic and trade disputes. Furthermore, or it may have different causal roles; in some cases, it may be proximate and powerful cause; in others, it may only be a minor and distant player in a tangled story that involves many political, economic and physical factors."[7]

After the end of the cold war and decreasing importance of geo-strategic considerations, the national security is being viewed in a comprehensive perspective. While there is no denying of the fact that the military dimensions of security are still relevant, there is an added emphasis on the non-military dimensions of security. Now it is not sufficient only to secure the territory and the sovereignty of the State but it is equally important to secure the people and his surroundings. It is in this perspective that a comprehensive view of national security has emerged which includes social, economic, environmental security along with the security of the state. Thus, both the military and non-military dimensions have become important in the changed framework of national security.

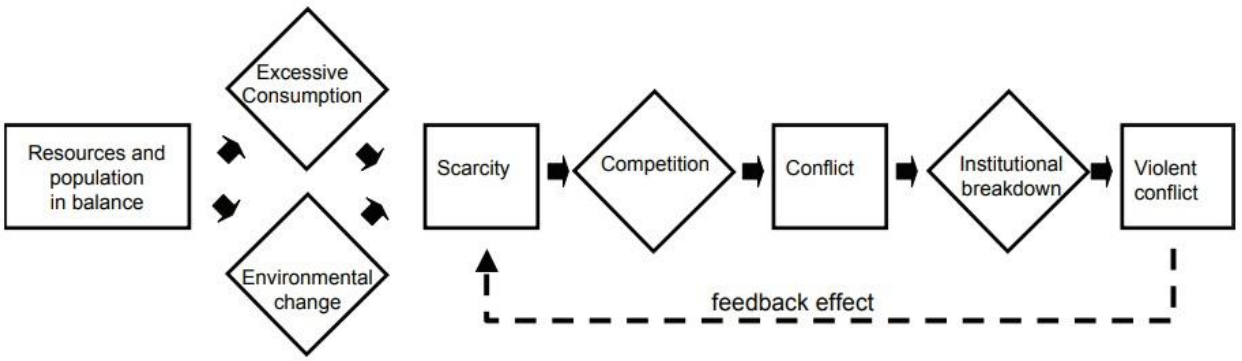
Environmental security reflects the ability of a nation or a society to withstand environmental asset scarcity, environmental risks or adverse changes, or environment-related tensions or conflicts. The chart below illustrates the potential for economic activity to cause environmental changes that lead to conflict.

Figure 1: Climate Change and Conflict



Unlike potential conventional military threats, these environmental threats are real and ongoing. However, not every environmental issue will result in a security problem, and most security problems are generated from complex situations involving environmental, political, social, and economic issues.

Figure 2: Common Conceptualization of Security Impacts of Climate Changes



Above figure suggests that when conditions of scarcity arise, through either increased consumption or climatic change, competition may emerge between users of scarce resources. Specific incidents that occur during this competition may give rise to a state of conflict between rival user groups. Where conflict resolution institutions and mechanisms fail, violence may result. A state of violence acts as a negative feedback mechanism on scarcity, since rival groups may increase their consumption of resources to complicate further the conflict, and refugees fleeing areas of violence may create new demands for resources elsewhere.

The comprehensive view of national security is based on the notion that it is not only the state alone which needs security but the people, the resources the socio-economic structures within

the state also need to be secured. In fact, now it is strongly believed that the security of the state is meaningless unless the people are secure. Therefore, some scholars have tried to define national security in terms of human security. The concept of human security gives the impression that the securing of human beings should not remain confined to the state boundaries. The comprehensive view of national security obviously includes social, economic, environmental security along with the security of the state. Thus, both the military and non-military dimensions are important in the changed framework of national security.

Climate Change and India's National Security

Climate change presents both direct and indirect threat to the security and stability of the society, state and the nation. According to estimation of IPCC, this century might see a rise of temperature from 0.30c to 6.40c. These changes in global temperature will affect all the spheres of life from food security, health, water availability to refugee problems, extreme weather conditions and conflict over resources that will lead to India's instability as well as threaten the national security.

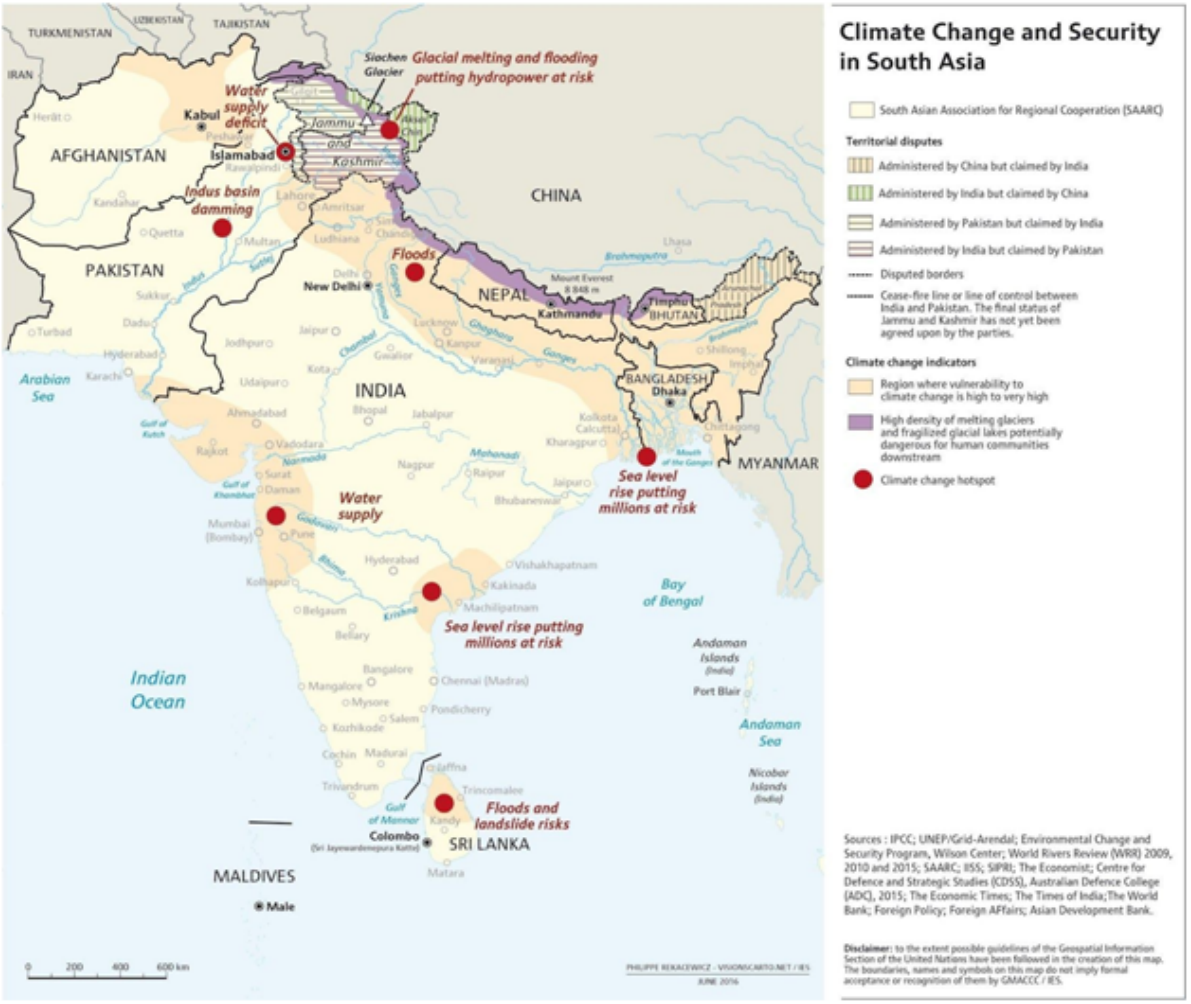
India has also not been spread the impact of climate change. The country which is home to 1300 million people has a high population density of about 350 persons per square km. It makes most areas of the country extremely vulnerable to various kinds of disasters which have bound to escalate with climate change. The country also has a long and populous coastline with a higher population density of 455 persons per square km. This coastal population depends heavily on the sea based livelihood sources and is highly vulnerable to various disasters originating in the sea. Such sea based disasters have only worsened in the last decade.

Following possible vectors through which climate change will impact national security include:

1. Melting of glaciers and Rising of sea levels
2. Decreased fresh water availability
3. Declining food productivity
4. Greater mass migrations and refugees
5. Health security
6. Energy crisis
7. Radicalism and Terrorism
8. Cultural Threats
9. Inter and Intra-state Conflict

Melting of Himalayan Glacier and Sea Level Rise: Impact on Cities

The two most relevant to the subject are the progressive rise in sea level and the increased intensity and frequency of climatic episodes leading to natural disasters due to the melting of Himalayan glaciers. Both represent significant threat to urban areas in developing countries. The fast melting of Himalayan glaciers due to climate induced global warming also present severe security challenges to India. In the north Himalayan glaciers are receding by about 16 meter every year. The receding glaciers have major implications for water availability in the glaciers fed rivers such as Ganga and Yamuna which serve as the main source of water supply to settlements along their banks.



Nearly 70 % of Earth's surface comprises of water in the form of seas and oceans. Sea level rise under warming is inevitable. Sea level rise is both due to thermal expansion as well as melting of ice sheets. According to several projections, the sea level is expected to increase anywhere from 8 to 88 centimeters during the 21st century, mostly due to thermal expansion and loss of mass glaciers and ice caps. The present scenario clearly indicates that the sea levels will definitely rise.[8]

Satellite observations available since the early 1990s show that since 1993, sea level has been rising at a rate of around 3 mm per year, significantly higher than the average during the previous half-century.9 IPCC predicts that sea levels could rise rapidly with accelerated ice sheet disintegration. Global temperature increases of 3–4°C could result in 330 million people being permanently or temporarily displaced through flooding. Warming seas will also fuel more intense tropical storms. With over 344 million people currently exposed to tropical cyclones, more intensive storms could have devastating consequences for a large group of countries. The 1 billion people currently living in urban slums on fragile Hillsides or flood-prone river banks face acute vulnerabilities. People living in the Ganges Delta and lower Manhattan share the same flood risks associated with rising sea levels.[10]

The coastal states of Maharashtra, Goa and Gujarat face a grave risk from sea level rise, which could flood land (including agricultural land) and cause damage to coastal infrastructure and other property. Goa will be the worst hit, losing a large percentage of its total land area, including many of its famous beaches and tourist infrastructure. Mumbai's northern suburbs like Versova beach and other populated areas along tidal mudflats and creeks are also vulnerable to land loss and increased flooding due to sea level rise. Flooding will displace a large number of people from the coasts putting a greater pressure on the civic amenities and rapid urbanization. Sea water percolation due to inundations can diminish freshwater supplies making water scarcer. The states along the coasts like Orissa will experience worse cyclones.

Climate Change Water Security

Rising air and water temperatures and changes in precipitation are intensifying droughts, increasing heavy downpours, reducing snowpack, and causing declines in surface water quality, with varying impacts across regions. Climate change worsens water quality and availability in India with water scarcity. Currently, 1.1 billion people are without access to safe drinking water11 and the situation is likely to be aggravated through climate change. Violence and disruption stemming from the stresses created by abrupt changes in the climate pose a different type of threat to national security than we are accustomed to today. Military confrontation may be triggered by a desperate need for natural resources such as energy, food and water. Depletion of aquifers in many parts of India and growing demand for water will bring agricultural, industrial, and urban use of water into conflict. This shortage will force water-usage restrictions and will increase the cost of water consumption. Water could become the "energy crisis" in the 21st century.

Increasing population in the region has put pressure on the land, agriculture and forest thereby putting pressure on freshwater for drinking, irrigation, industries and habitation. Conflicts over water will grow over the coming decades as growing populations demand more and climate change affects supply. With the overwhelming majority of the world's rivers shared by two or more nations, these challenges will test diplomats and political leaders worldwide.[12]Some South Asian countries are in water crisis. The quantitative supply problems are increasing. It is estimated that India will enter the stress zone by 2025, where the per capita water availability fell from 6000 cubic meters in 1947 to 2300 cubic meters in 1998.Freshwater availability in India is also a concern; available water is expected to decrease from 1,820 m3 per capita to < 1,000 m3 by 2025 in response to the combined effects of population growth and climate change.[13] Estimates for the year 2050 predict an acute shortage of water in India, Pakistan, Sri Lanka and Bangladesh shortly after 2025.[14] The receding trends of some glacier masses could threaten water supplies, livelihoods and the economy of the region. Richard Damania warned that in the long term, there can be no replacement for the water provided by glaciers, and this could result in water shortages at an unparalleled scale.[15]

In India, the major river systems of the Indian sub-continent namely- Brahmaputra, Ganga and Indus which originates in the Himalayas are expected to be more vulnerable to climate change because of substantial contribution from snow and glaciers into these river systems.[16] Studies have shown that increase in the temperature by 1.50c will increase the risk of some floods in the Ganga and Brahmaputra plains.[17] A warmer climate could cause a reduction in water availability in summer. The Ganga, Brahmaputra, and Indus may soon become seasonal rivers, dry between monsoon rains if Himalayan glaciers continue their retreat. Water labels will continue to fall. An action Aid study has shown that water levels in almost all streams in Kashmir valley have fallen by 2/3rd and ground water levels have dropped by more than 1/3rd .These problems are occurring due to the receding glaciers. The gross per capita water availability in India will decline by over one-third by 2050 as rivers dry up, water labels fall or grow more saline. Water scarcity will in turn affect the health of vast populations, with a rise in water-borne diseases such as cholera. Other diseases such as dengue fever and malaria are also expected to rise.[18]

Thus, reduction of arable land, widespread shortage of water, diminishing food and fish stocks, increased flooding and prolonged droughts are already happening in many parts of the South Asian region. Water shortage has the potential to cause civil unrest and lead to significant economic losses, even in robust economies. The consequences will be even more intense in areas under strong demographic pressure. The overall effect is that climate change will fuel existing conflicts over depleting resources, especially where access to those resources is politicized.

Agriculture and Food Insecurity

Another major threat that climate change poses to the country is through its impact on agriculture. Since agriculture is a source of livelihood for 65 percent of the population and contribute to 27 percent of the GDP, adverse impact on agriculture would have serious effect on the economy of the country. In addition it will also have an impact on food security and health. It has been estimated that 0.5 degree rise in temperature would result in reduction of wheat yields by 10 percent. However, the loss of crops and agricultural land due to disaster intensification and land degradation caused by climate change cannot be estimated. The extreme weather events that have occurred in the country are already reeling under the impact of climate change.

Rural areas are still home to some 72% of India's 1.1 billion people, most of who are poor and marginalized and rely on agriculture as their main source of income.[19] As large parts of the arable land in India is rain-fed, the productivity of agriculture depends on the rainfall and its pattern. Agriculture will be adversely affected not only by an increase or decrease in the overall amounts of rainfall but also by shifts in the timing of the rainfall. Any change in rainfall patterns poses a serious threat to agriculture, and therefore to the economy and food security.

Global climate change (GCC) is likely to increase food demand by around 300% by 2080 because of higher population, higher income, and demand for biofuel; and this rise is likely to create an imbalance between food supply and demand even without the effects of GCC and, as is expected, if there is a decline in food production due to GCC, it is likely that there will be more crises over food supply and demand, and a relentless rise in prices, threatening food security.[20]

A drop in agricultural productivity will lead to, or worsen, food-insecurity in Indian subcontinent and an unsustainable increase in food prices sweeping. It has been called the 'silent tsunami.' In these countries, a sharp drop in food crop production could lead to internal strife across urban-rural and nomadic-sedentary cleavages.[21] If environmental degradation makes food supplies increasingly tight, exporters may be tempted to use 'food as a weapon'.[22]

The impacts of climatic change on potential rice production, as studied by the International Rice Research Institute indicate that increasing temperatures may decrease rice potential yield up to 7.4 percent per degree increase in temperature,23while wheat production could fall by 32% by 2050.[24] India ranks number one among countries that rely on rainfed agriculture, in both size (86 million hectares) and value of production to the country[25].Rainfed agriculture alone accounts for roughly 44% of total food grain production in India[26]. Therefore, a more volatile monsoon season could be damaging to a significant piece of India's agriculture and food supply.

The changes in rainfall pattern and distribution owing to climatic change can lead to shifting of agricultural lands and may also force intensive cultivation of marginal lands which in turn will exacerbate deforestation in future. All these can have tremendous impact on agricultural production and hence food security of any region. Equally important determinants of food supply are socio-economic environment policies, capital availability, prices and returns, infrastructure, land reforms and inter and intra national trade that might be affected by climate change. Climate change could ultimately cause the gradual impoverishment of societies in this region, which could aggravate class and ethnic cleavages, undermine liberal regimes, and spawn insurgencies.[27]

Thus, the scarcity of productive agricultural land and decline in agricultural production seem to be two important reasons for inducing cross border migration in India. One study suggests that the number of people crossing over to India increases during periods of environmental disaster.[28] If these situations continue unabated, the volume of migration from affected countries will increase in the future.

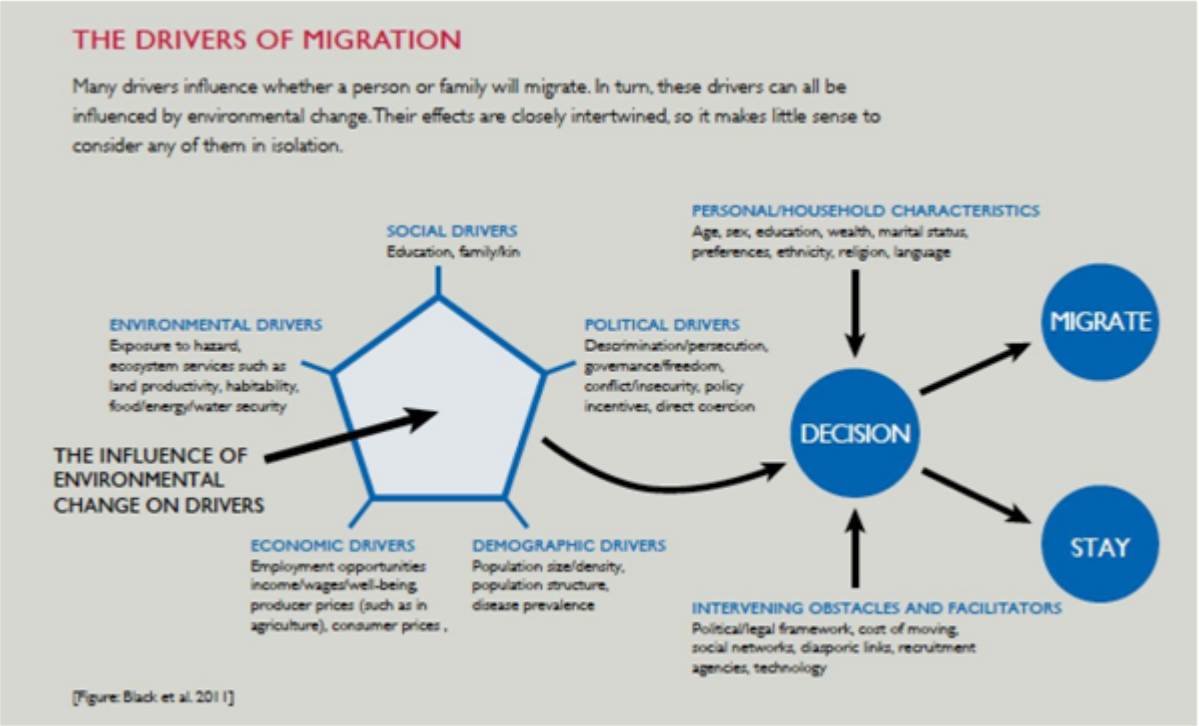
Human Displacement or Migration

The implication of large-scale population migration is another India's national security issue that could be exacerbated by climate stressors. Changes in local and regional climatic conditions in the form of sea level rise, heat stress, desertification, flooding and drought severely restrict livelihood options for large groups in developing countries. On the one hand, these changes may directly challenge basic subsistence of already disadvantaged communities in the region, thereby further increasing their vulnerability across social, economic and institutional settings. On the other hand, increasing local vulnerability could potentially trigger large-scale internal displacement and migration in search of new avenues for employment and settlement that can further lead to destabilization and violence. Such destabilization may take place at various levels: local (group vs. group), national (group vs. state) and international (state vs. state) level.

The increasing sea levels as well as more extreme weather conditions will force millions of people to migrate, potentially leading to higher pressures on resources in areas of destination and subsequently to resource competition and possibly political instability and violent conflict. According to Dr. Tobias Feakin, "Climate change poses a complex security challenge in the form of forced migration and resource based conflicts."[29]

The potential for large-scale migrations of people – both within countries and across borders – has been described as 'perhaps the most worrisome problems associated with rising temperatures and sea levels which could easily trigger major security concerns and spike regional tension.'[30]

According to Goodhart, international migration produces social stability risks, leads to demographic security, creates cultural identity issues and poses a threat to social security system and welfare state philosophy and generates many internal security challenges. Bulging populations and land stress may produce waves of environmental refugees,[31] that spill across borders with destabilizing effects on the recipient's domestic order and on regional stability. The National Defense University, published in the New York Times in August 2009, explored the potential impact of a destructive flood in Bangladesh that sent hundreds of thousands of refugees streaming into neighboring India, touching off religious conflict, the spread of contagious diseases and vast damage to infrastructure.[32] Indicating the severity of the problem , Mr. A. J. Dory, the US Deputy Assistant Secretary of Defence for Strategy commented that "it gets real complicated real quickly."[33]



Due to migration of refugees, the ethnic and social divide manifested in the state between various groups causing political and civil strife and conflict in society. This gravest problem has been faced by India from last twenty years. Environmental degradation as well as population pressures on scarce natural resources in Bangladesh has contributed to a large scale migration of Bangladeshis to the north-eastern states as well as to some of the large urban centers in India. Though the exact number of migrants from Bangladesh to India is difficult to assess, about 12-17 million Bangladeshis were estimated to have migrated to India by the year 1993. In 2003, India has about 20 million Bangladeshi migrants to neighboring West Bengal and Assam and various parts of India,[34] 2.2 million Nepalese, 70,000 Sri Lankan Tamils and about 100 thousand Tibetans.[35] James Hansen, the director of the NASA Goddard Institute for Space Studies, has estimated that all of

Bangladesh's population of 144 million people could become climate refugees by the end of the century. [36] Presently, this migration is limited not only to Assam, Tripura and West Bengal but is to far-off states like Tamil Nadu, Maharashtra, Gujarat and Delhi.[37] This phenomenon has generated a host of destabilizing political, social, economic, ethnic and communal tensions in many states and union territories of India.

It is alleged that this migration has not only environmental base, instead they are induced to cause premeditated population imbalance on religion line. Assam's ethnic strife over the last decade has apparently been provoked by the migration from Bangladesh.[38] In many instances the immigrants have benefited at the cost of the development of the original inhabitants thereby leading to adverse social, economic, environmental and political impacts. The migrants have also been regarded as a security threat by the intelligence agencies in India for their susceptibility to getting involved in information gathering activities for extremist groups both on the India- Bangladesh border and on the frontier with Pakistan.[39]

The volatile situation in Assam as well as the approaching saturation point in West Bengal has led to large-scale migration to the large urban centers like Delhi, Mumbai and Hyderabad. The migrants have become a part of the local political struggle in many areas, with a potential for violent conflict. To some political parties in India, the migrants have been a tool to enlarge the political base either by winning their support or by mobilizing the native Hindu population against the Muslim immigrants. Within Bangladesh, in the Chittagong Hill Tracts, south of the north-eastern Indian state of Tripura, an ethnic conflict rages between the Bengali speaking Muslim population and the native Buddhist and Christian tribal population of the thinly populated but densely forested area. The ensuing clashes have transformed into insurgency operations involving the Bangladeshi military forces.[40]

On the other hand the subversive elements are being pushed by ISI in the garb of environmental migrants to implement its sinister design of 'Greater Bangladesh.' It is a challenge for India to manage its borders. In this situation, it is the first and foremost duty of our leadership to take concrete action to secure our frontiers and sub-serve the best interests of the country.

Health Security

Climate change poses a host of threats to the survival of mankind. The debilitating impact of climate change has broadened the sphere of discourse much beyond the traditional concern like environment or development. Climate change has a direct impact on human health. Impacts from climate change on extreme weather and climate-related events, air quality, and the transmission of

disease through insects and pests, food, and water increasingly threaten the health and well-being of the Indian people, particularly populations that are already vulnerable. For example, the warmer the climate the likelihood of its impact on human health becomes worse. Available studies suggest that there will be an increase in health problems. It is anticipated that there will be an increase in the number of deaths due to greater frequency and severity of heat waves and other extreme weather events. Each year, about 800,000 people die from causes attributable to air pollution, 1.8 million from diarrhoea resulting from lack of access to clean water supply, sanitation, and poor hygiene, 3.5 million from malnutrition and approximately 60,000 in natural disasters.41 A warmer and more variable climate would result in higher levels of some air pollutants, increase transmission of diseases through unclean water and through contaminated food.

Current climatic conditions heavily impact the health of poor people in developing nations, and climate change has a multiplying effect. It is estimated that the health of 235 million people a year is likely to be seriously affected by gradual environmental degradation due to climate change.42 This is based on the assumption that climate change will increase malnutrition, diarrhea and malaria. Malnutrition is the biggest burden in terms of deaths. Climate change is projected to cause over 150,000 deaths annually and almost 45 million people are estimated to be malnourished because of climate change, especially due to reduced food supply and decreased income from agriculture, livestock and fisheries.

A greater understanding of the relationship between climate variability and human health in a country such as India could aid in the development of new prevention strategies and early warning systems, with implications throughout the developing world. Future studies must work to more explicitly define the relationship between climate variability and emerging and reemerging infectious diseases such as dengue, yellow fever, cholera, and chikungunya virus[43] as well as chronic diseases related to cardiovascular and respiratory illness, asthma, and diabetes. Millions of people below the poverty line and those in rural areas represent high-risk populations who are exposed to myriad health risks, including poor sanitation, pollution, malnutrition, and a constant shortage of clean drinking water. However, as awareness and public health infrastructure increase, the burden of climate-related disease may be negated.[44]

Energy Crisis

Over the coming decades, the world faces a daunting challenge in meeting growing global energy needs while mitigating the impacts of global climate change. In view of the predicted climate trends and their associated socio-economic processes, key infrastructures are facing new

demands. Climate induced consequences negatively affect the key infrastructures and make it more vulnerable which has wide ranging security implications such as:

1. The impacts of climate change may damage key infrastructures, such as energy supply, and consequently destabilize public order.
2. Wide-ranging destruction of the coastal infrastructure may lead to mass migration movements and trigger tensions in regions of destination.
3. The decline in hydroelectric power generation may additionally reinforce competition/conflicts over fossil energy sources.

The impacts of climate change may damage key energy infrastructures, such as energy plants, energy routes, nuclear installations, and consequently destabilize public order. The decline in hydroelectric power generation may additionally reinforce competition and conflicts over fossil energy sources.

Radicalisation and Terrorism

Radicalization and terrorism may be increased in many developing societies due to the climate induced social and economic deprivation. Many developing countries do not have the government and social infrastructures in place to cope with the types of stressors that could be brought on by global climate change. When a government can no longer deliver services to its people, conditions are ripe for the extremists and terrorists to fill the vacuum. The radical and terrorist exploit this condition as a recruiting ground by offering various social services to the people. An April 2007 report by the Military Advisory Board of the CNA Corporation, a US-based think tank, seeks to make explicit the link between climate change and terrorism. T. J. Lopez states in the report that 'climate change will provide the conditions that will extend the war on terror'.[45] This statement is based on the premise that greater poverty, increased forced migration and higher unemployment will create conditions ripe for extremists and terrorists.[46] Although there is a well-established link between economic disadvantage and civil unrest, this does not necessarily manifest itself through terrorism Lebanon's experience with the militant group Hezbollah and Maoism or Naxalism in India are glaring example of how the central governments' inability to provide basic services has led to the strengthening of a radical organization. Resource scarcity could be a contributing factor to conflict and instability.

Cultural Threat

Climate change can jeopardize the cultural heritage of people and society. As people are losing their homes and livelihoods, increasing number of people are becoming climate refugees - leaving their history and tradition behind. It is predicted that some of the endangered groups in North-East which are coming under further stress due to climate impacts will disappear in the future, thereby posing a threat to the cultural security of the society and the state.

Inter-state and Intra-state Conflicts

Climate induced insecurities can trigger interstate and intrastate tensions and conflicts. States may be stressed to the point of collapse. The potential for regional conflicts due to climate induced condition will be extremely high. It is very clear that armed conflicts are often caused by disputes over shared resources and struggles over these resources are often the result of population depletion, degradation, or unsustainable use. At the most basic level, we all depend on the natural environment for our survival. It is the sole provider of the most basic of human needs: food, water and shelter. Global warming and the resulting changes in the environment will affect our ability to meet these needs. Conflict as a result of climate change is likely to emerge if the carrying capacity of the land is overwhelmed, or as a result of competition over specific resources.

Measures taken by India:

International Level:

India is a party to UNFCCC as well as Kyoto Protocol at the international level. As emission of greenhouse gases is the key factor for climate change, and developed countries contributed more in this, it was considered the responsibility toward cuts in greenhouse gas emissions. It was an active player in the creation of UNFCCC and Kyoto Protocol. It represented the voice of developing countries at the international level, but the recent rise in its greenhouse gas emission due to industrialization process, putting pressure on it to change its position (Sengupta 2012).[47] It still speaks the language of no commitment on GHG as it needs to build industries for poverty eradication and developed countries should play their part out of historic responsibility. Until Copenhagen India was successful in its attempt on principle of differentiation. United States wanted to erase these clauses in specific and Kyoto protocol in general. India with the help of Brazil, China and South Africa resisted this move. But climate regimes were weaken in 2010 at Cancun agreement.

Domestic Level:

At the same time India established a Prime Minister's Council on Climate Change (PMCCC) to evolve a coordinated national-level response to this issue in 2007 at the domestic level. The purpose of this council was to provide oversight on key policy decisions. Next Year government launched a National Action Plan on Climate Change (NAPCC), containing 'eight national missions', with the aim of addressing climate change in a manner that would also generate development 'co-benefits' (Government of India 2008, Cited in Sen Gupta 2012).[48] These eight national missions are as follows:

1. National Solar Mission: deploy 20,000 MW of solar electricity capacity in the country by 2020.
2. National Mission for Enhanced Energy Efficiency: new institutional mechanisms to enable the development and Energy Efficiency strengthening of energy efficiency markets.
3. National Mission on Sustainable Habitat: it focuses on the promotion of the introduction of sustainable transport, energy-efficient buildings, Sustainable Habitat and sustainable waste management in cities.
4. National Water Mission: integrated management of water resources and increase of Mission water use efficiency by 20 per cent.
5. National Mission for Sustaining the Himalayan Ecosystem: observational and monitoring network for the Himalayan the Himalayan Ecosystem environment so as to assess climate impacts on the Himalayan glaciers and promote community-based management of these ecosystems
6. National Mission for Green India: afforest an additional 10 million hectare of forest lands, wastelands and community lands
7. National Mission for Sustainable Agriculture: enhancing productivity and resilience of agriculture to reduce vulnerability to extremes of weather, long dry spells, flooding, and variable moisture availability.
8. National Mission on Strategic Knowledge for Climate Change- challenges arising from climate change, promotes the development Knowledge on Climate Change and diffusion of knowledge on responses to these challenges in the areas of health, demography, migration, and livelihood of coastal communities

Suggestions

India will have to devise its strategies carefully to mitigate these challenges. On the one hand, it will have to resist the international pressure on it to take binding objections with regard to CO_2 emissions as this will seriously affect the prospects of economic growth. On the other, it will have to undertake suitable adaptive measures to ensure that its economic growth is based on sound principle of energy efficiency resource conservation. As India is being labeled as a significant emitter, it will also have to craft its Negotiating position carefully to safeguard its national interests without being isolated.

At this juncture of history, it needs to be recognized that environmental crisis potentially has more pervasive and more security implications than any other crisis. For this reason, environmental challenges should be placed at the core of security considerations in a rapidly changing world. Hence, effective international cooperation should occur to address the unpredictable consequences of climate change. It is undoubtedly true that development rarely takes root without security; it is also true that security does not exist where human beings do not have access to enough food, or clean water, or the medicine they need to survive. This is why the world must come together to confront climate change. There is little scientific dispute that if we do nothing, we will face more drought, famine and mass displacement that will fuel more conflict for decades. 'We need to rethink about 'security'. The threat of climate change is not one that can be met or managed through traditional military security. Armies cannot be amassed, barriers cannot be built and weapons cannot be deployed against a threat that is indiscriminate and global in its scope. We need to move towards the idea of 'sustainable security'.

Conclusion

India, as a developing country is facing and will face many problems in development. National disasters which results from climate change will put a burden on its development and progress. India has been a key factor in international politics from global and its needs to maintain that position, otherwise it will not be able to garner the support for the change in policies which affect climate change. India should strengthen the regional collaborative mechanisms as part of our national strategy on climate change. The defence cooperation between the militaries of the region should focus on creating joint parallel command structures to facilitate a synergized response in the wake of a natural or a man made calamity. These mechanisms should also be effectively interfaced with the UN agencies and other non-governmental organizations operating in the region. As an emerging great power, India should be seen leading this initiative but this collaborative mechanism

should not be at the cost of millions of our citizens. Greater collective ambition is the need of the hour to tackle global warming.

It cannot be wished away and we are already playing a 'do nothing' climate tax on our economy and environment. Indeed if 'we are the first generation to feel the effect of climate change and the last generation that can do something about it we must meet the climate century head on. It's time to get moving on climate action. If not now, When? Thus, the need of the hour is of a collective vision, a vision of a world where we are able to coexist with nature giving back as much as we take, Jonathan Swift said it best when he said, and "Vision is the art of seeing things invisible". It is the collective responsibility of the Parliaments to make this invisible apparent and tangible for the masses to follow. The risks can no longer be hushed up, nor ignored. Then alone, could we make some headway in saving our lone planet from the brink of climate disasters.

References:

1. https://www.justsecurity.org/63673/climate-change-our-greatest-national-security-thre at/
2. http://sustainablesecurity.org/article/assessing-security-challenges-climate-change| May 2011
3. http://www.thedailystar.net/newDesign/news-details.php?nid=198040
4. http://www.thedailystar.net/newDesign/news-details.php?nid=198040
5. http://www.ipcc.ch/pdf/glossary/ar4-wg1.pdf, 942
6. Holland and Vagg, "Global Security Defense Index on Climate Change" March, 2013.
7. http://americansecurityproject.org/featured-items/2013/the-global-security-defense-in (accessed April 11, 2014).
8. Thomas F Homer-Dixon, "On Threshold: Environmental Changes as causes of Acute Conflict," International Security, Vol.16, no.2, 1991, p.77
9. An Assessment of the Intergovernmental Panel on Climate Change: Climate Change 2007: Synthesis Report, p. 20
10. IPCC Fourth Assessment Report, p. 11
11. UNDP Human Development Report 2007-2008, p.78
12. German Advisory Council on Global Change, 2008.
13. http://www.un.org/popin/cenasia/faotex3.htm
14. IPCC Report 2007 andhttp://www.pacinst.org/topics/environment
15. http://static.teriin.org/energy/envsec.htm#water

16. http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:22404173~pagePK:34370~piPK:34424~theSitePK:4607,00.html
17. V. K. Sharma, Global Warming: Its Impact on India, Indian Institute of Public Administration, New Delhi, (2008) p.17
18. Ibid
19. The Hindu, 18 April, 2007
20. World Bank 2009.
21. Ibid.
22. Hindol Sen Gupta, Not war, but climate change might devastate South Asia, Fortune India, 13 June, 2019
23. Sarfaraj Alam, Environmentally Induced Migration from Bangladesh to India, Strategic Analysis, vol.27, No.3, Jul-Sep.2003, p.433
24. Peter Wallenstein, "Food Crops as a Factor in Strategic Policy and Action," Westing, Global Resources, pp. 151-155
25. Ibid. p.146-151
26. www.epa.com
27. www.fao.com
28. Sharma, Bharat et al. Vittal, K.P.R. "Estimating the potential of rainfed agriculture in India: Prospects for water productivity improvements" Science Direct (2010)
29. Sharma, Bharat et al. Vittal, K.P.R. "Estimating the potential of rainfed agriculture in India: Prospects for water productivity improvements" Science Direct (2010)
30. The Times of India, November 20, 2007
31. R.A. Warrick, R.M. Gifford, and M.L. Parry, "CO2, Climatic Change and Agriculture: Assessing the Response of Food Crops to the Direct Effects of Increased CO2 and Climatic Change," in Bert Bolin, et al, (ed). The Greenhouse Effect, Climatic Change, and Ecosystems, SCOPE No. 29 (New York: Wiley, 1986), pp. 393-474
32. One World South Asia, 29Nov. 2009
33. Kurt M Campbell et al, The Age of Consequences: The Foreign Policy and National Security Implications of Global Climate Change(Washington DC: Centre for Strategic and International Studies/Centre for a New American Security, 2007, p.8)
34. Ted Gurr, "On the Political Consequences of Scarcity and Economic Decline," International Studies Quarterly, Vol. 29, No. 1 (March 1985), pp. 51-75 Jodi

35. Jacobson, Environmental Refugees: A Yardstick of Habitability, World Watch Paper No. 86 (Washington, D.C.: World Watch Institute, 1988.
36. Obayedul Hoque Patwary, Assessing the Security Challenges of Climate Change http://sustainablesecurity.org/article/assessing-security-challenges-climate-change May 2011
37. Ibid
38. The Hindustan Times, January 3, 2003. NTS bulletin, no.1, 2008 www.rsis-ntsasia.org
39. Uttam K. Sinha, Environmental Stresses and their Security Implications for South Asia, Strategic Analysis, vol.30, No.3, Jul-Sep.2006, pp.609
40. Myron Weiner, "The political Demography of Assam's anti-immigrant movement", Population and Development Review, vol.9, no.0, June 1983, pp.279-292) http://www.thesouthasian.org/archives/000113.html
41. Gurneeta Vasudeva, Environmental Security: A South Asian Perspective, Tata Energy and Resources Institute, 1600 Wilson Boulevard, pp.19-20.
42. http://rajyasabha.nic.in/rsnew/publication_electronic/climate_change_2008.pdf
Human Impact Report, Global Humanitarian Forum, 2009
43. Shope R. Global climate change and infectious diseases. Environ Health Perspect. 1991; 96:171–174.
44. Dhiman R. C, Pahwa S, Dhillon GPS, Dash AP, Climate Change and the Threat of Vector-borne Disease in India: Are We Prepared? Parasitol Res. 2010;106:763–773.
45. National Security and the Threat of Climate Change, (CNA Corporation, 2007), p.17.
46. Ibid.
47. Ibid.
48. https://www.iiste.org/Journals/index.php/IAGS/article/view/39157/40266

Removing Border in South Asia: Challenges & Opportunities

Mr. Manojit Das
Research Scholar
Department of Political Science
Goa University
Email: hi.monojitdas@gmail.com

Abstract:

SAARC's progress for achieving its aim has always been halted due to border and other minor issues among the member nations. The member nations have spent too much on their defense forces for maintaining human created borders forcing a shift in focus from development to defense. The region being a pool of talent, resources are drained by other super powers for their need. Today in the age of cyberspace, SAARC must try and attempt to find a solution to its long term issue of insecurity that exists in the region, especially between its two big brothers India and Pakistan to make the region a cyber power in current digital world. Unlike other arenas cyberspace does not have any contention over the boundaries, neither in sharing of resources as it is open to all. This paper will explore the challenges and opportunities of cooperation that member nations have in cyberspace overcoming natural constraints that are imposed by physical barrier, to initiate friendship and mark a new beginning.

Introduction

On 8 December, 1985 South Asian nations Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan and Sri Lanka finally decided to create SAARC (South Asian Association for Regional Cooperation) which aimed at developing the region as one regional unit. The initiative was spearheaded by Zia Ur Rahman, former President of Bangladesh.[1] The group launched the Integrated Program of Action (IPA) which included five areas for immediate cooperation viz agriculture, rural development, telecommunications, meteorology, health and population activities, later transport, scientific and technological, sports, postal, arts and culture were added to the list.[2] Afghanistan joined the family in 2005. The region has 9 (nine) observers namely (i) Australia; (ii) China; (iii) European Union; (iv) Iran (v)Japan; (vi) Republic of Korea (vii) Mauritius (viii) Myanmar and (ix) United States of America.[3] SAARC family's two elder brothers (India and Pakistan) are mainly responsible for ensuring the annual meeting to happen as tension between brothers led to cancellation of many annual meets. The boundary issues prevented several annual

meetings like 1989, 1992, 1994, 1996, 1999, 2000, 2001, 2003, 2006, 2009, 2012, 2013, 2015 and 2016 over fear that India and Pakistan may go for war. Other issues like Jammu & Kashmir and Teesta River water sharing, raises the tension between India-Pakistan and India-Bangladesh respectively besides several other small issues among member nations becomes hindrance in achieving aim. India being in the geographical centre and bigger in terms of landmass has land boundary with almost every member nation (except Afghanistan) in the region making it normal to have more issues with other members in terms of border. This tension is quite a normal phenomenon as we see it even in our family when it comes to distribution of property among the children since this region is comprised of a single landmass with close cultural bond. In SAARC's case the division was not created by grandfather but by British rulers who ruled the region thereby keeping the door open for conflict always as it is hard to decode their complex industrial technologies and strategies even today. It is quite clear that they never wanted the region to be united again so as to keep an option for them to return to the region for ruling them as advisors or modern day "consultants".

Humans' increasing urge for technology and dependence on cyberspace has been felt in South Asian region like the rest of the world but impact is in higher ratio as compared to the rest of the world as population is high in the region where it is slowly making it an eternal part of humans in the real world with its direct attributions. The advancement of cyberspace has not only made work easy but created a sense of threat if that good is used by the negative thinking groups or people to implement their version of good.[4] Cyberspace is now included in the list of the domain of war front and it is actively taken into consideration when framing the national defense policy or plan.

Challenges of South Asia

The region which creates high technologies and raw materials lives on low income in comparison to other nations which earns profit from that produce. It is a well accounted fact that much before European Economic Community came into existence in 1958[5], the three south Asian nations viz; Bangladesh, India and Pakistan were doing better business until 1947, till they were together. After 1947 partition in the region with the birth of India and Pakistan, things reversed with the increasing violence in the region, the violence since then is providing benefit(s) to other nations such as USA, Russia, China etc. China who has a keen interest in the Indian Ocean has managed to gain key ports in Bangladesh, Pakistan and Sri Lanka. The region which produce similar crops are more in competition with each other on items like tea, jute, rice creating more adversaries than friends who unite in creating rice stores at different places for better income.

Like the other nations of the world, the SAARC member nations after fighting several wars and destroying resources for the maintenance of human created border, find it almost impossible to remove the political border as nations have spent too much on its defense forces for the contradictions or rifts that exists over boundary issues. Even the tensions that are arising in the region has active element of cyberspace in it as the non state actors from Pakistan who intrude inside India are using this cyberspace feature to create problems. It is purely impossible today to even think of intrusion/ attack without involving electronics specially cyberspace to its advantage. Other scenario where the countries rises against each other include the Fake Currency Notes, money laundering, smuggling, human trafficking which are carried via cyberspace communication. Can the unlawful activities be carried so effectively in today's time without cyberspace? The answer is no! Even the human trafficking which is a big threat to the region involves cyberspace as the dealings will require internet since devices are being purchased by security agencies to snoop on mobile conversations via IMSI tracker devices.[6]

The import and export items among the SAARC nations itself faces a challenge. Apart from raw materials and crops, important items like electrical machines, faces the threat of being dual use spy device, thus making a nation to reject the device on ground security concerns. India and Pakistan has mastery in the region for using their indigenous technology to their advantage, when the same is modified for exporting to generate revenue, the neighboring nations don’t trust thinking that the equipment may be spying object specially designed by the nation's intelligence agency for surveillance. This spy culture has to give due credit to cyberspace media and the Chinese masterminds; the Chinese have made it possible to hack into every technological device that can be connected to the internet with Huawei being the commander probably of the electronic chip force as Huawei have left no stone unturned to spy on US and other nations where ever it exports equipments.[7] The propaganda in internet which spreads any skillfully designed rumors in such manner that truth seems to be the main culprit in the event. There are several initiatives undertaken by the member nations to become self sufficient but still the finished product has to be exported to non member nations which are away from the region for this negative environment. This is why powerful nations have been able to establish their presence in the region through their private owned companies like HP, Microsoft, Bosch and carry their business successfully.

There are N numbers of SAARC origin people especially from Bangladesh, India and Pakistan who are now face of big global brands and well established in their lives away from the region. Their economic assets are high in the world where US $ still acts like a dictionary and translator when a nation's currency is converted to other. And even after this the HNWI (High Net

Worth Individuals) are increasing in the South Asian region with Bangladesh being ahead of not only other Asian nations but many other wealthy nations making it in the top 10 list of nations with spending wealth.[8] The US $ role as dictionary has to be removed in SAARC region if the economy boost is given a thought, doing this in the real world is almost impossible as member nations won't agree in designing single currency stating their role must be highlighted in the designing of currency, but this same can be sorted in virtual mode when a digital payments App can be designed to carry monetary transactions in the region. A digital payments app can be designed in association with the principal banks of all partner nations and all regional payments can be made so as to remove not only US$ from the region but boost the payments system whenever US$ makes any nation to crumble with decreasing value against US$. Google's payment App now has a base of 50 million users in India[9] and they are distributing 102 INR for its promotion when a user refers it another user. Why is Google being so generous towards India is it simply because it has Indian connection or because to get access of the Aadhaar linked details of every individual as Hon'ble PM of India took initiative to make it compulsory to link the bank account and other utilities with Aadhaar card[10] to calculate the unaccounted wealth an individual has stored. Google a US based company through its distribution of money is luring youngsters (tomorrow’s leaders) with 100 INR and securing their details is definitely an attempt by big power to track active surveillance so that tomorrow's leader can be better understood today only. In the same way region receives funding from other nations and in turn sign/share the crucial areas of their national important.

The student or people here in SAARC region fear to interact with neighboring friends not only in real but in virtual world fearing that Government agencies may come and pick them up for interrogation because agencies cannot catch actual cyber criminal due to lack of coordination and instead catch innocent victims. Even for top officials who hold good portfolio and wants peace in SAARC region like PM Modi, PM Hasina, PM Imran, Sardar Sidhu are termed as traitors from both the sides due to their friendly attitude. But the happiest part is today's young generation go abroad for studying especially back to rulers of their mother/fatherland (Britain) prefers staying in same apartment and sharing meals. After course gets completed many prefer to stay back in there because of the open society and in case few returns the intelligence guns must have activated the vigilance mission on the student especially for cross border cyberspace communications. There is an urgent need for initiating confidence building measure at the student level in the digital domain where students can really help in decreasing gap in distrust among member nations. Youth of the region who are more virtually connected with the world, must be given the platform to get united to revive the old rich heritage and how to make the region the wealthiest empire. The trust deficit among the

members are growing day by day due to groupism where one nation is joining hand with other to make itself feel secure but in actual they are making themselves weak by exposing the vulnerabilities and flaws. In the content the external involvement like China and US are biggest threats not only in technology but in physical world; if trades are taken into account then individual trade ties with china is seen to be more of member nations that among themselves.

The problem that persists today are improper land demarcation, illiteracy, food scarcity, insecurity, poor hygiene and sanitation can be tried to solve by the cyberspace awareness where Apps can help in educating people about actual land demarcation and create awareness about identifying fake news to stop regional hatred. SAARC satellite has already been launched for enhancing regional cooperation[11] but a ground level design to cater to the youth welfare for knowledge sharing has to be developed and border area challenges like where farmers/ fisherman cross illegally can be guided using cyberspace. These are not impossible as the same regional youth are going abroad and designing these technologies using cyberspace for other nations who in turn are going to sell it to the region. Areas where the borders are close and people generally cross due to easy access of local healthcare system can be made to register under cyberspace based App system so that doctor appointment and other necessary facilities can be provided to ease the issue and eradicate the concern of illegal migration; In similar way the illiteracy issue in remote areas near borders can be solved by internet based apps and smart learning centers which can be developed under BADP (Border Area Development Plan) and in other areas under SAARC development plan. The involvement of local politics into framing the foreign policy of nations gives a big challenge for the SAARC when issues like Indus water sharing, Teesta water sharing, Madheshi people and Tamil ethic issues made relations between India-Pakistan, India-Bangladesh, India-Nepal & India-Sri Lanka a little tough. The actual scenario doesn't have any link with cyberspace but the effects were felt when the patriotism of the people rises up and people abuses and hurls each other for the act which ultimately modifies the actual content of the issue. The SAARC proposes for development in regional with better connectivity and connected roads/ other network but it is always opposed by stating threats to national security. The use of technology can be used for moving the trade and smart security systems can be designed to remove threats. Development should not be halted stating security as concern instead advancement has to be made to crush the threats.

The ideology of India's "Vasudhaiva Kutumbakam" is probably more challenged in cyberspace as for visiting India's land mass people will need a passport and today a confidence is there that the fake passport can be identified; when intrusions are carried out in data servers of India it does not need a passport to access and sometimes create a great loss. The concept of "Vasudhaiva

kutumbakam" was coined much before and there was no stealth technology or Stuxnet virus present. Today to make the nation a real secure it is important to secure the nation's border followed by its regional border and especially the cyberspace.

The Indian Cyber Army and Pakistan Cyber Army, computer hacking groups who are always behind each other defacing and stealing resources from each other's Government or crucial establishments[12] can actually think sometimes of preventing attacks from threats originating outside the region and aimed at them. Because they are not the only enemy of each other, other nations too have interest in their national politics; these two nations are being targeted by giants for selling their finished products too, if tension is eased between the brothers of region who will purchase costly weapons from other nations. USA being much cyber advanced nation become failure to prevent data breach then individual nations of the region are an easy prey to such attacks. The Chinese hackers who are responsible for USA's largest data breach OPM attack is definitely behind its Asian competitor India for similar hacking and similar data base in the name of UIDAI. Pakistan may take that China would not take any interest in Pakistan's data because they are all weather friend, but it's quite true only national interest matters and why China is not attacking Pakistan because China has easy access to Pakistan’s data server due to close involvement between the two. When India and Pakistan will be busy attacking each others’ server, any tech giant can come in to take the collected data and use it to their advantage therefore it is better to identify common goals and enemy.

Development by a member in the region is definitely contested with same development in the nation so that deterrence can be maintained, while maintaining deterrence the domain which actually needed resources are left deprived. This debate of development v/s defense is an unending event and cannot be resolved in a simple article but the topics which can be resolved with a little effort like collaboration in cyberspace, where the intelligence of regional talents can make the SAARC cyber power. If history of becoming nuclear power of both India and Pakistan to be looked once, it is very clear that despite of super power & their super spy elements the nations were able to make themselves nuclear power with utter determination and skills. Today at this same situation when the virtual world is being dominated by giants then why not join hands and make SAARC a cyber power where threats are to be answered jointly.

The road ahead

All modern threats to the nation like Counterfeit note, smuggling, radicalization and other things like spreading of rumors are mostly carried out through cyberspace, therefore real time collaboration is most crucial in order to prevent it than investing it after the event. Messaging app

WhatsApp came in India with active measure to counter rumour by putting limitation for forwarding a message up to next 5 contacts. But Indians effectively came out with several tricks to bypass the checks by forming a chain from every next 5 contacts, it is because the whole region is full of household talents which cannot be confined with small checks.

To boost the trade and bring economy regional virtual E-Commerce stores like Alibaba needs to be designed which will help in selling the regional exports to the world. This will fetch good revenue and a small share of profit can be donated to the regional poverty eradication.

The pool of talents in SAARC can be only be made to come out through cyberspace where individuals can present their ideas, because seminar/events will also not be able to accommodate everyone. Thereby the ideas might be missed and when these clusters of small ideas go abroad they become loss for the region.

Student exchange facilities at virtual level to be acknowledged and encouraged so that scholars can really express themselves and learn more about the region. SAARC University established at New Delhi is not capable to accommodate all keen students and besides money being a factor in organizing it but in cyberspace a forum can be initiated to ensure that these young minds can stay active and share their ideas which can be of immense help in solving the long standing tussle between the regional members. The youth today are the future leaders of tomorrow, today's youth are more inclined towards cyberspace in order to bring in a peaceful and secure future we need an association not merely through any of the United States made WhatsApp group or Facebook page where again an involvement of foreign nations comes in later paving way for disagreements in the cyberspace level too, emphasis can be laid in making an application based architecture so that it can be accessed at ease as youths are working mostly on smartphones, also government can take responsibility of ensuring that they provide much needed security to the platform so that it can stay safe from evil keystrokes of foreign nations preying on the platform.

It is never to be forgotten that the internet may come at a cheaper price making it so appealing and addictive but the price which users are paying much more than money, it is their personal information which is collected by gangs/groups and then sold to third party companies who uses for generating revenue either by providing to government or to business industries for being used in various purposes ranging from political campaigns to selling of product and much more. SAARC virtual channel in TV, radio can also be established wherein students can share their ideas for regional harmony. Like all other inventions created for regional integration ranging from SAPTA to SAFTA which faced a lot of challenges,[13] cyberspace also faces same heat which is basically a reflection of imagination and thoughts of real world individuals. There are surveys

available on the internet which provide details about all member nations and an even mention on the amount of data consumed on which applications, this survey may be looked as normal for the sake of data but in turn raises a concern that it means in this USA dominated world when using every results we are looking at their place nothing is hidden from them that is why they are able to provide the data of searched keywords and most visited sites, who knows they might know what content we have searched on that site. There are many information getting exposed everyday which shows how vulnerable and helpless we users are, a need can be moved on in growing for a regional search engine in order to filter and apply additional layer of security to prevent data brokers from coming in between and keep an eye on the proceedings made on that website.

Involvement of big players, who are ever ready to extend their helping hand in designing the cyberspace apex body should be avoided in order to make the region devoid of Trojan horse of big powers. India has established cyber security centre in Hyderabad in partnership between the Government of Telangana and Hague Security Delta (HSD) working in securing critical infrastructures, government network with team comprising of more than two dozen companies always ready to support and ensure secure cyberspace for the local business and companies. Pakistan has established its own National Centre for Cyber Security at Air University, Islamabad with the aim of protecting Pakistan's cyber space and helping its national companies who are dependent on cyberspace. Indian venture which has already involved non regional players and Pakistan surely will slowly be inviting senior faculties and experts from China as visiting fellows making it China's international cyber station as China and its technology already have managed to spread its presence across the globe to ensure that they have access to every data.[14] China has not left its own citizens i.e. Uyghur Muslims from surveillance conducted with high precision using cyberspace and AI shows it's cautiousness on national interest[15] as Uyghur has been a concern for the PRC China always, therefore Pakistan bringing in China is always like opening a backdoor and simultaneously India inviting other nations are definitely a step which will create more rift and distance in achieving regional unity. Although the step of establishing HSD in India and NCCS in Pakistan will not be opposed in any case by any technical giants or nations it is not because they are supporting the two giants in South Asia for achieving big feat in cyberspace but these two big players in the regions are creating vulnerabilities for the outsiders to involve and take driver's seat in deciding the future of the region.

To ensure the impact of real world effect is not shared in the virtual world as region being highly patriotic won't be able to control its anger when any little issue takes place in the real world between the member nations.

The proper framing of policies for sharing of resources in virtual world depending upon requirement else it may trigger the feeling of biased attitude leading to real world scenario of giving birth to inseparable element called distrust/

A joint cyberspace venture cUNSA (cyber United Nations of South Asia) can be designed comprising the member nations and Bangladesh, India, Pakistan taking main leadership overcoming their attitude of attacking each other and removing the inseparable element called distrust among themselves. The cyber body can help member nations to become cyber equipped preventing foreign nations to come into the region for guiding with technical advancements and also prevent attacks from China, Russia, USA and other superpowers who want to colonise cyberspace. The common aim of data security and integrity makes all member nations to stand united in this digital era and secure the interest of combined South Asia together.

The hope for new beginning

MJ Akbar, current Indian government minister said "we cannot change too much of our past, but can change a substantial amount of future", PM Modi of India said "Nation's destiny is linked to its neighborhood". Senior Vice President (SVP) of SAARC Chamber of Commerce and Industry (Pakistan) Iftikhar Ali Malik highlighted newly elected PTI regime of PM Imran Khan's wish of playing a constructive role to strengthen SAARC by bringing India and Pakistan together. He further said "The region accounts for only three percent of global output and two percent of world exports, it is better to collaborate than unhealthy and non productive competition. Bangladesh PM Sheikh Hasina's continuous motivational words "SAARC has not been ineffective, the eight nation regional body is very much alive and it has opportunity to do more work for changing the lot of the people of South Asia".

The above leaders give us hope that there can be collaboration in the region in actual which will definitely lead to the region becoming a global superpower if they take nation and region to be their priorities. The progress has to be devoid of hidden trojan horses which are generally accompanied in this region due to insecurity.

India now started focusing on cyber security and have conducted cyber exercise among all its security agencies like National Security Council Secretariat (NSCS), National Technical Research Organisation (NTRO), Computer Emergency Response Team – In (CERT-In), Defence Research and Development Organisation (DRDO), National Informatics Centre (NIC) and representation from academia and IT industry similarly this same initiative can be taken at the regional level with involvement of security agencies, academia and the IT industry of member

nations to really track the perpetrator and not accuse each other when actual incident happen. The cyber exercise can be made fruitful only when nations send its expert not on recce mission of knowing the other members cyber arsenal for waging cyber war upon return but to learn and plan for fighting jointly when any crisis arises to the region.

To understand the real potential of SAARC, an online match between gamerz of SAARC and the world can be arranged to see the talents. Arranging a cricket match between SAARC XI and World XI is definitely possible as Afghanistan and Nepal now has specialist bowlers and batsman who can dominate any team while organizing this in real may be a costly affair with complications but arranging this in highly secured virtual platform won't be that difficult if the tasks are handed over to the cyber hackers of the region for preventing intrusions in the game. The online players can make their presence felt to the world with their keystrokes.

Conclusion

With current leaders of the region expressing desire for cooperation and identification of avenues, member nations can go through joint ventures and cooperation via cyberspace with each other for the price fixation will avoid the exploitation by big powers.

The current leadership who are active in cyberspace needs to take the initiative so that things can actually come into effect, three big regional powers leader are highly tech savvy as PM Modi with his thoughts on social platform Twitter and dependence on Aadhaar, newly elected PM of Pakistan Imran khan has used the cyberspace completely to his advantage with App designed with name Constituency Management System (CMS)[16] which comprised of database of voters. The app was so effective which is why Imran Khan is now PM Imran Khan. PM Sheikh Hasina of Bangladesh is also active Twitter user and her country is the biggest victim of cyber attacks in recent past with attacks in its bank.[17]

The initiatives taken at national level must be extended to regional level in order to achieve desired target, with radicalization in full swing in the region and recent attack in Sri Lanka on auspicious day of Easter again highlights the need. The alleged suicide bomber Zahran Hashim used social media to gain thousands of supporters and motivated them to hate the non-Muslims through his Youtube and Facebook account under the name of Al-Ghuraba Media and his affinity towards Daesh dates back to 2017 when he started posting and sharing few Daesh propaganda video.[18]

It is normal to say that India and Pakistan are big brothers in the South Asian family and India being eldest in research did announced that the Government of India has designed two new divisions for dealing exclusively with online radicalizations and cyber crime naming it as Counter

Terrorism and Counter Radicalization (CTCR) division and Cyber and Information Security (CIS)[19] as many of India's youth mostly from Kerala have left to join Islamic State due to online radicalization. Indian government did share with Srilanka about a possible attack before the Easter bombing but it was not dealt seriously and since another brother Pakistan who has a strong connection there among the Srilankan Muslims due to Pakistan's mission of "inflicting India with 1000 cuts" did not tried to prevent this as it might have proved India's superiority in acquiring intelligence in the region and deny Pakistan the status of cyber superpower in the region. Pakistan who spends more time in gathering information of Indian military through their camouflaged apps made available on Google Play store[20] and both nations using their experts with website defacing knowledge including stealing data from each other's server over each other could have easily joined to save the younger brother Sri Lanka and many innocent lives in the island nation.

Now time stands when just a Whatsapp share and Facebook post is capable of creating nationwide strike and chaos has not been to instigate the need of a cyber forum for mutual intelligence sharing, at least preventing terrorists organization like Daesh / ISIS in taking innocent lives and coming in race of being cyber power in the region although being an external actor.

The ISIS and ISIL has announced through its Amaq News Agency on May 10, 2019 that they have established their presence in India to conquer the South Asian region with the name of "Wilayah of Hind", or Province of Hind, and claimed to have already made presence felt by killing few security forces of India deployed in Kashmir region of India[21] . The news may be perceived by Pakistan as happy moment to cherish but it has to be remembered that ISIS are working both on virtual and real world making it lethal force and also there is a possibility that it will start hacking few sites of India first and then initiate cyber war between India and Pakistan later resulting violence in Kashmir and damage could be faced more by Pakistan as Pakistan does not have too fortified defence in cyber and security force. The time has finally come to show maturity for the member nations by working collectively and start framing policies freshly in this new domain as it is the nation's politics that decides the fate of the region. If member nations work together for the region then the day is not far when SAARC will become a cyber power; with secure cyberspace the member nations will also have a secure nation as internet and cyberspace are only means of information sharing and gathering now which eventually also become an example for other organizations to follow in the digital world.

Footnotes

1. SAARC SECRETARIAT. (2018). Retrieved from http://www.saarc-sec.org

2. SAARC: Main Objectives of SAARC. Ghai, K. (2018). Retrieved from http://www.yourarticlelibrary.com/economics/trade-economics/saarc-main-objectives-of-saarc/40408
3. Ghosh, P. and Das, M. (2017). Camouflage Warfare of Modern Era- The Future of Modern Warfare. Indore: Shiva Prakashan, pp.30-51.
4. The history of the European Union - 1958 - European Union - European Commission. (2018). Retrieved from https://europa.eu/european-union/about-eu/history/1946-1959/1958_en
5. Brewster, T. (2016). For $20M, These Israeli Hackers Will Spy On Any Phone On The Planet. [online] Forbes.com. Available at: https://www.forbes.com/sites/thomasbrewster/2016/05/31/ability-unlimited-spy-system-ulin-ss7/#43d733ba63fa [Accessed 20 May 2019].
6. Keane, S. (2019). The Huawei controversy: Everything you need to know. [online] CNET. Available at: https://www.cnet.com/news/the-huawei-controversy-everything-you-need-to-know/ [Accessed 20 May 2019].
7. The Daily Star. (2019). Bangladesh to see 3rd fastest rise of the rich. [online] Available at: https://www.thedailystar.net/country/news/bangladesh-3rd-fastest-growing-country-rich-population-report-1689829 [Accessed 20 May 2019].
8. Akolawala, T. (2018). Google Tez UPI-Based Payments App Reaches 50-Million Downloads Milestone. Retrieved from https://gadgets.ndtv.com/apps/news/google-tez-upi-based-payments-app-reaches-50-million-downloads-milestone-1886883
9. Next on Modi's list? Mandatory Aadhaar linkage with property. (2018). Retrieved from https://www.google.co.in/amp/s/m.economictimes.com/news/economy/policy/modis-big-move-on-real-estate-mandatory-aadhaar-linkage-with-property/amp_articleshow/61738772.cms
10. South Asian Satellite to boost regional communication. (2018). Retrieved from http://pib.nic.in/newsite/printrelease.aspx?relid=161611
11. The India - Pakistan cyber war intensifies with ransomware attack. (2018). Retrieved from http://www.dailymail.co.uk/indiahome/indianews/article-4082644/The-India-Pakistan-cyber-war-intensifies-retaliatory-ransomware-attack-cripples-websites-Islamabad-Multan-Karachi-airports.html

12. Hirantha S.W .From SAPTA to SAFTA: Gravity Analysis of South Asian Free Trade. Retrieved from https://www.etsg.org/ETSG2004/papers/hirantha.pdf
13. Danielle Cave, E. (2019). Mapping China's Tech Giants. [online] Aspi.org.au. Available at: https://www.aspi.org.au/report/mapping-chinas-tech-giants [Accessed 20 May 2019].
14. Cimpanu, C. (2019). Chinese company leaves Muslim-tracking facial recognition database exposed online | ZDNet. [online] ZDNet. Available at: https://www.zdnet.com/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/ [Accessed 20 May 2019].
15. Saad Sayeed and Drazen Jorgic, R. (2018). How a phone app served up Imran Khan's Pakistan election win. Retrieved from https://www.livemint.com/Politics/DLCfHgRsV460Ox4PcRfNQM/How-a-phone-app-served-up-Imran-Khans-Pakistan-election-win.html
16. Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat | Reuters. (2018). Retrieved from https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH&grqid=6cXCkmEm&s=1&hl=en-IN
17. Arab News PK. (2019). How Zahran Hashim went from obscure extremist preacher to the alleged mastermind of the Sri Lanka bombings. [online] Available at: http://www.arabnews.pk/node/1488261/world [Accessed 20 May 2019].
18. Jain, B. (2017). Home Ministry: MHA forms two new divisions to check radicalisation, cyber fraud | India News - Times of India. [online] The Times of India. Available at: https://timesofindia.indiatimes.com/india/mha-forms-new-divisions-to-check-radicalisation-cyber-fraud/articleshow/61595400.cms [Accessed 20 May 2019].
19. Cimpanu, C. (2016). SmeshApp Removed from Play Store Because Pakistan Used It to Spy on Indian Army. [online] softpedia. Available at: https://news.softpedia.com/news/smeshapp-removed-from-play-store-because-pakistan-used-it-to-spy-on-indian-army-501936.shtml [Accessed 20 May 2019]
20. Bukhari, F. and Pal, A. (2019). Islamic State claims 'province' in India for first time after clash.... [online] Reuters. Available at: https://www.reuters.com/article/us-india-kashmir-islamic-state/islamic-state-claims-province-in-india-for-first-time-after-clash-in-kashmir-idUSKCN1SH08J [Accessed 20 May 2019].

Terrorising Myths

Mohit S. Purohit
Researcher,
Kanhoji Angre Maritime Research Institute
Email: mr.mspurohit@gmail.com

Abstract

The article will discuss the everyday myth in the sense of something that's not shown to be true by empirical or scientific evidence. One relys heavyly on media that portrays a certain kind of an image of terrorism. Terrorist cases often attract a huge amount of attention internationaly, but then when a large number of terrorism cases are considered carefully, one develops an image quite different from that of the stereotypes.

Introduction

The article is about common myths about terrorism and stereotypes that we developed because of the Black Swan nature of terrorist attacks. That is the tendency for people to be overly influenced by a few high profile attacks, like the 26/11 attack or other Black Swan attacks like those that have happened in the last couple of decades in Madrid, in London, in New York, and Oslo. The idea is that these very high profile attacks get a huge amount of press, but they may not hold up when we look at their characteristics across all terrorist attacks. In this case using the Global Terrorism Database or the GTD, a dataset that assist empirical analysis of over 113,000 attacks around the world.

Method

Analysis is based upon a large number of cases, in doing so the article rely on a database that is called the Global Terrorism Database, or the GTD. It contains data from 1970 to 2012, over 113,000 terrorist attacks from around the world. Another source is Global Terrorism Index, referred in the article as GTI. The article will mainly talk about 26/11 and 9/11 as an example.

Literature

Why do stereotypes have such an important impact on the society? Nassim Nicholas Taleb, a renowned satistation, defines an event as a Black Swan incident in his book with the same title. If something falls outside the realm of regular expectations, has a high impact. The term is based on the observation that before Europeans visited Australia, they had assumed that all swans were

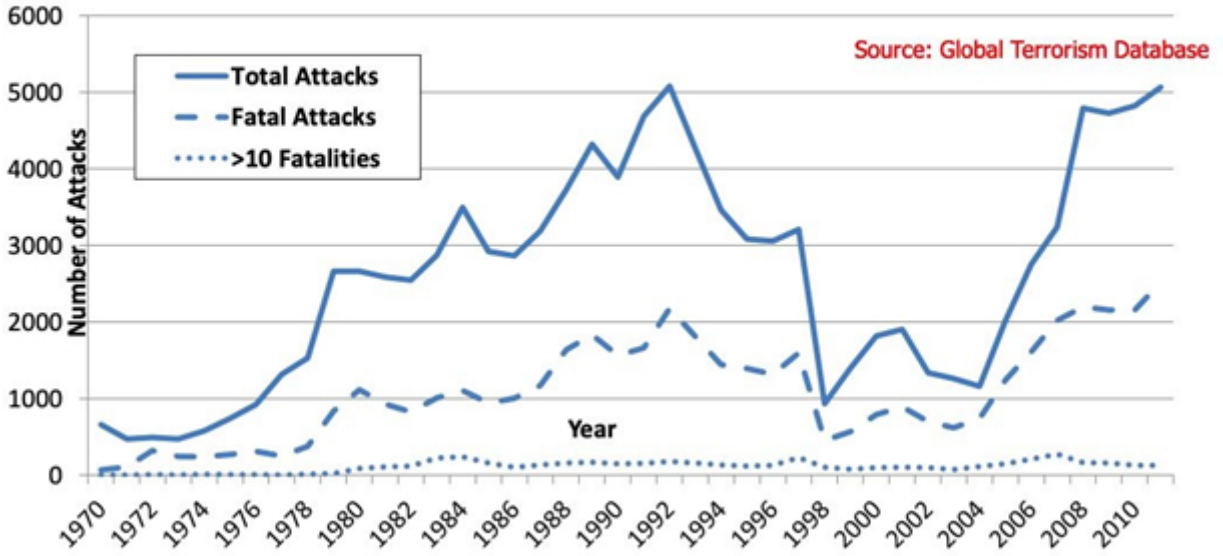
white. An assumption that fits their experience. It was not until they arrived in Australia and were able to witness black swans. Based on Taleb's example, one can safely claim that the coordinated attacks of 26/11 are a perfect example of a Black Swan Event. Because the events were unexpected, it had a huge impact on history, and the attacks were difficult to predict in advance. So, stereotypes usually affects one's image of terrorism, it may produce an incorrect assumptions about terrorism. The Black Swan idea fits in, even though they're not typical at all of the underlying reality, they can have a huge impact.

Myths in the society

The article will focus on some of the stereotypes exist in society because of the black swan nature of terrorist attacks. Then compare those stereotypes to the findings in greater detail at how those attacks compared to many attacks around the world. Going all the way back to 1970 shall dismantle the idea of how one sees an act of terriorism. This phenomenon is not just true for terrorism, it's true for a range of criminal actions.

1. The article will discuss nine myths. The first of these myths, is that **the Terrorist attacks were rapidly increasing in the years leading up to 9/11**. All the publicity generated by an attack like 9/11, it's easy to think that it was representing a kind of big upsurge in terrorist attacks. It was arguably the most pronounced of such attacks. Other countries have suffered similar tragedies. For example, the London 7/7 attacks in 2005 on the tube and transport for London, the attacks on the train system in Madrid on 11/03/04, attack in Oslo on 22/07/11, etc. All of these attacks generated a huge amount of publicity, which can have a Black Swan effect. In other words, they contribute to stereotypes about terrorism, when they may not quite live up to these stereotypes.

Worldwide Terrorist Attacks, 1970-2011



According to the data, terrorist attacks actually reached their 20th century highpoint not in the years leading up to 9/11, but after. There was a major increase in terrorist attacks in 1992, just after the collapse of the Soviet Union. Total attacks the year before 9/11 were actually at about the same level as they had been in the mid-1970s. In the four years prior to 9/11, worldwide terrorist attacks were at their lowest level in about 20 years. Since 9/11, attacks have been increasing dramatically.

2. Myth number two. **Terrorist attacks reach every corner of the world.** The fact that we live in such an interconnected world, where media is present even in relatively isolated and faraway places, gives the impression that terrorism is happening everywhere and that it could happen anywhere.

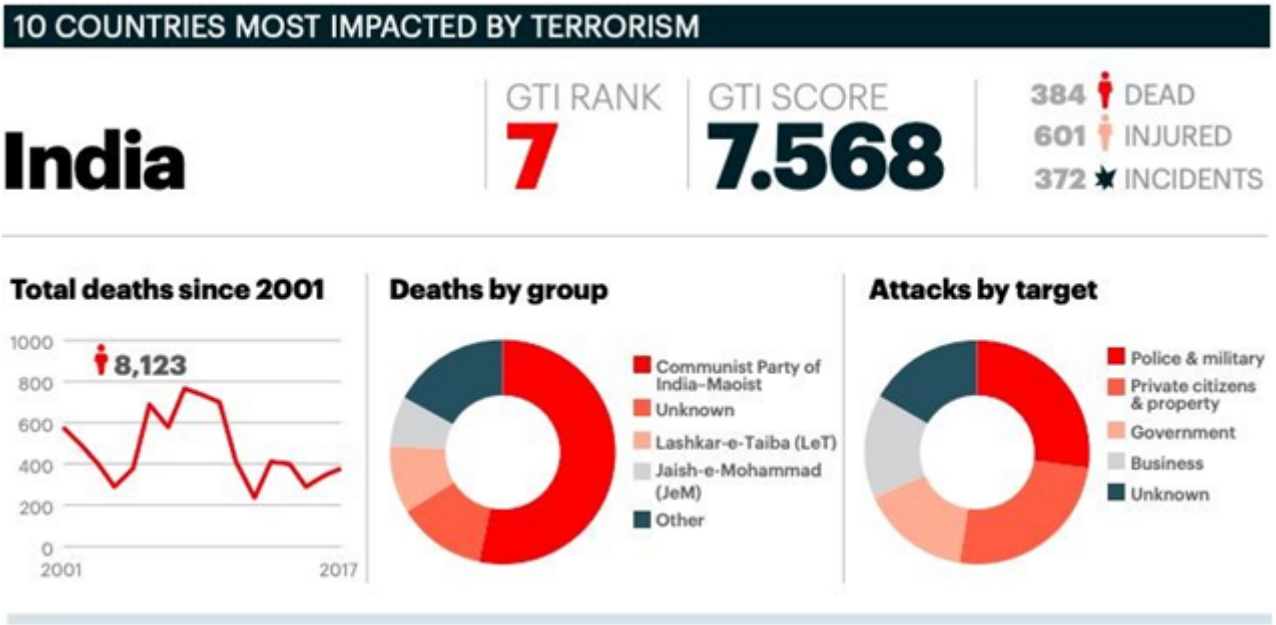
Top Ten Countries for Terrorism, 1970-2010

Source: Global Terrorism Database

RANK	COUNTRY	CUMULATIVE % OF ALL ATTACKS	CUMULATIVE % OF ALL COUNTRIES
1	COLOMBIA	7.32	0.48
2	IRAQ	13.92	0.96
3	INDIA	20.15	1.44
4	PERU	26.31	1.92
5	EL SALVADOR	31.74	2.40
6	PAKISTAN	36.26	2.88
7	NORTHERN IRELAND	40.22	3.37
8	SPAIN	43.49	3.85
9	PHILIPPINES	46.74	4.43
10	SRI LANKA	49.72	4.81

However, the data suggests, terrorist attacks tend to be highly concentrated. The blanket media coverage then gives an incorrect idea that no place on the planet is really safe. The GTD indicates that terrorist attacks happen in relatively few places. For example, the top ten countries, in terms of terrorist attacks, account for nearly half of all terrorist activity in the world. So, about 5% of all countries in the world account for more than 50% of all terrorist attacks. If we look at 10% of the countries of the world, it accounts for 75% of the world's terrorist attacks. So, terrorism tends to be highly concentrated. There are many parts of the world where terrorist attacks are very unlikely.

3. Myth number three. **India is more frequently targeted by terrorists than any other country in the world.** It applies especially to 26/11 because it received so much publicity, not just in India, but in many parts of the world.



According to GTI, India ranks about 7th in the world. Total attacks is 866 and 384 fatalities in 2018. Fatalities in India have been on a downward trend since they peaked in 2008 at 775 deaths. The most frequently attacked country according to the data set is Iraq, and Afghanistan recorded the most number of terrorist fatalities.

Ten countries most impacted by terrorism, ranked by number of deaths

In 2017, Afghanistan recorded the highest number of deaths from terrorism globally for the first time since 2012.

Country	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Afghanistan	43	24	16	6	14	10	6	3	4	3	3	3	3	3	1	2	3	2	2	1
Iraq	19	17	30	29	24	2	1	1	1	1	1	1	1	1	2	1	1	1	1	2
Nigeria	24	15	57	35	23	17	18	29	7	14	18	6	11	4	4	4	2	3	4	3
Somalia	43	28	21	35	28	24	32	30	20	5	5	7	7	6	7	6	6	8	6	4
Syria	43	54	57	51	52	41	29	44	31	46	27	56	50	11	5	5	5	4	3	5
Pakistan	9	7	12	13	10	9	5	6	6	2	2	2	2	2	3	3	4	6	5	6
Egypt	27	45	57	51	52	41	16	10	21	46	53	47	50	18	24	11	19	7	13	7
Congo, DRC	15	30	15	23	22	12	23	22	18	15	7	4	10	14	15	17	15	14	9	8
Central Afr. Rep.	43	54	57	51	52	41	40	44	45	38	46	19	17	33	46	18	9	20	17	9
India	3	2	1	3	3	1	4	2	3	4	4	5	4	5	8	7	13	15	12	10

Source: START GTD, IEP Calculations

4. Myth number four. **Most terrorists attacks involve disgruntled groups and individuals from one country attacking civilians in another country.** The 26/11 attacks, along with some of the other high profile attacks, like those of the Twin Towers in New York, Madrid train and London transport. They often involve a situation where individuals from one country come to do serious damage to another country. So, that makes it an international attack. But, how common are these international attacks? For researchers, it has been very difficult to figure this out until quite recently because none of the major databases that have studied terrorism, let alone distinguish between domestic and international attacks.

In an analysis of terrorist attacks in the GTD, a very large proportion of attacks involve domestic assailants, domestic groups, attacking domestic targets. The scope of violent instances in India is particularly broad, with 51 different terrorist groups being responsible for at least one terrorist attack in 2017 and 25 groups being responsible for at least one terrorism death.

The deadliest domestic group in India is the country's communist party - Maoists. The Maoists, otherwise known as the Naxals, were responsible for 205 deaths and 190 terror incidents in

India, or 53 percent of deaths in 2017. The group has been active for several decades with 2010 its deadliest year on record. Maoist frequently stage attacks against the Central Reserve Police Force (CRPF) and other armed forces throughout the country's northern and central territories.

The north Indian state of Jammu and Kashmir had the most deaths in 2017, with 102 deaths committed by five different international terror groups, most notably Lashkar-e-Taiba (LeT), Jaish-e-Mohammad (JeM) and Hizbul Mujahideen (HM). Lashkar-e-Taiba, the most active Islamist terror group in India, was responsible for 10 percent of deaths in 2017. The same group was also responsible for 26/11 terror attacks in Mumbai. The remaining 37 per cent of terror deaths were committed by 21 different groups, further highlighting the wide distribution of domestic (insurgents) and international (terrorist) groups in India.

5. Myth number five. **Terrorism is unrelated to traditional political grievances.** If you take an attack like 26/11, which seem to be so irrational, which seem to have the characteristics of nothing that could have been done to negotiate or to prevent it, where the goals of the perpetrators were not even entirely clear, it's easy to think that all attacks have political grievances that are hard to sort out.

Top Twenty Perpetrator Organizations: Total Terrorist Attacks, 1970 to 2011

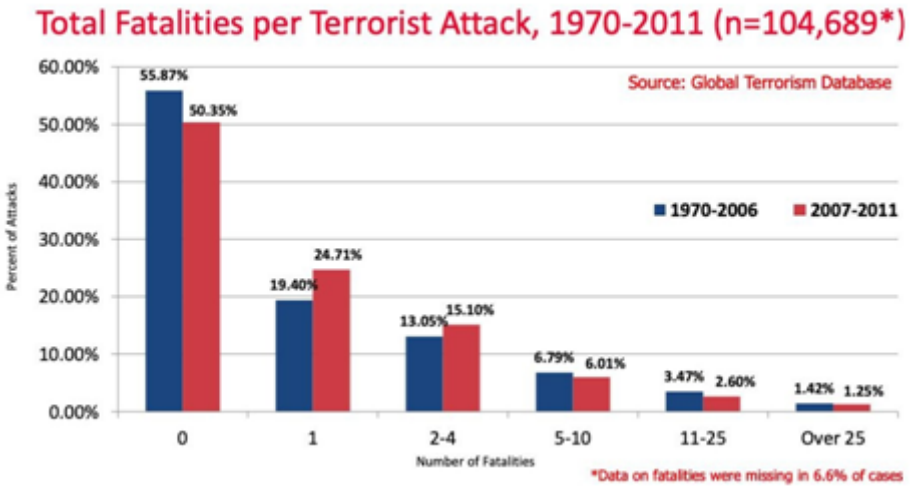
	Perpetrator Group	Attacks	Fatalities
1	Shining Path (SL)	4518	11570
2	Farabundo Marti National Liberation Front (FMLN)	3351	8065
3	Irish Republican Army (IRA)	2673	1809
4	Revolutionary Armed Forces of Colombia (FARC)	2045	5240
5	Taliban	2030	5770
6	Basque Fatherland and Freedom (ETA)	2027	818
7	Liberation Tigers of Tamil Eelam (LTTE)	1606	10946
8	Communist Party of India - Maoist (CPI-M)	1416	1889
9	New People's Army (NPA)	1335	3438
10	National Liberation Army of Colombia (ELN)	1292	1469

Source: Global Terrorism Database

Above are the top ten terrorist organizations in the world between 1970 and 2012. Now, how many of these organizations actually have a specific political agenda? It could be an organization such as ETA, that wants its own homeland in a particular part of Spain and France, or it could be an organization like the FMLN, that's trying to take over an entire country for a particular group. Nonetheless, they tend to have fairly specific political agendas, often based on the idea of trying to

develop a homeland for a particular group. So, these do not seem to be unrelated to political grievances, but are certainly very political.

6. Myth number six, is the idea that **most terrorist attacks are incredibly lethal.** The terrorist attacks are most likely to receive publicity. They seem to be highly lethal and certainly events like 26/11, and the likes in Madrid, in London, and in New York, it is easy to suppose the terrorist attacks are incredibly lethal. However, the data as a whole if we look at all 113,000 cases we find that more than half of all terrorist attacks since 1970 involved no fatalities.



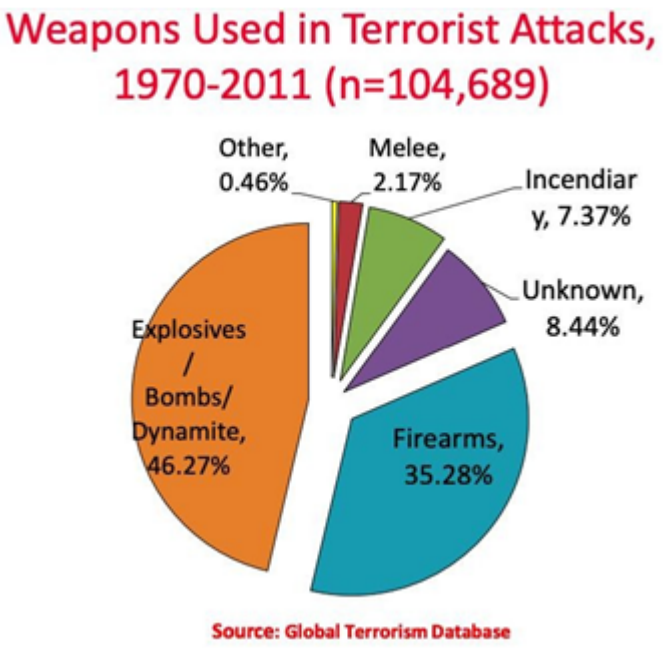
One wonders, how can it be that so many terrorist attacks did not result in fatalities. There are several reasons, the first and the most obvious is sometimes terrorists don't plan for fatalities. Sometimes they are directing their efforts to destroy property. The attacks are on facilities, could be on bridges, on electric structures, on factories, and so on. Many of the attacks by environmental groups like the ELF, or animal rights groups like the ALF, have been of this type. They target particular kinds of institutions, not at the individuals who maybe in them.

It can also be the case that attacks are aimed at civilians but they fail. Terrorist organizations plan to take the lives of individuals, or plan to reduce individuals to casualties, but they just are not successfully doing this. Lastly, in many other cases, terrorists are not trying to kill individuals, even though they set up situations that could lead to the death of individuals. For example, in the 1970s and early 1980s, it was common for groups like ETA, the IRA, the Red Brigades to warn people before their attacks, before they set bombs off, so that individuals would not in fact be killed in the attacks. This kind of thinking and act led terrorism researcher Brian Jenkins, to suggest that "terrorists want a lot of people watching, not a lot of people dead."

Now, half of the attacks, about 50,000 attacks in the GTD produced at least 1 fatality. It's also the case that nearly 2% of the attacks in the database, about 1,200 attacks, produced more than

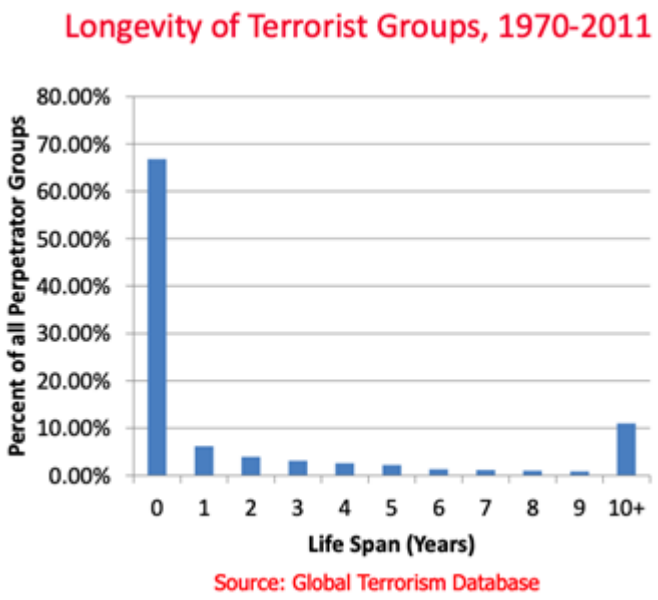
25 fatalities over a 40 year period. Brian Jenkins revisited his earlier statement after considering this as a very serious problem. After reviewing, he has revised his statement to say, “many of today's terrorist, not only want a lot of people watching, but a lot of people dead.” Nevertheless, about half of all terrorist attacks since 1970 recorded in the GTD produced no fatalities.

7. Myth number seven, **most terrorist attacks rely on sophisticated weaponry.** If you think about the coordinated attacks of 26/11 and 9/11 which involved split second timing, long term planning, a very innovative use of a particular kind of technology that was used in an extremely destructive way. It is convincing to think all act of terrorism involve highly planned, very sophisticated attack patterns. If one also considers how terror is portrayed by the international film industry and media, one realises the reality of 26/11 attack is nothing compared to the kind of attacks shown in the movies and television series. So these images encourage us to think that most terrorist attacks depend on sophisticated weaponry and split-second long-term planning. Contrary to this view of terrorism, a vast majority of terrorist attacks rely on non-sophisticated, readily accessible weapons. According to the GTD database, 80% of all attacks rely on explosives and firearms which are among the most accessible weapons. The explosives used are relatively calm, the most common one is being dynamite and grenades. Similarly, the most common firearms are readily available including shotguns and pistols. So sophisticated weapons, chemical weapons, biological, radiological, nuclear weapons are rare exceptions.



8. Myth number eight, **most terrorist organizations are long-lasting and difficult to eradicate.** Given the persistence of groups like Al-Qaeda, the ETA, the LTTE, the FARC, the IRA. It appears likely that all terrorist organizations are long lasting and very difficult to eradicate. In reality, some of these organizations have been around for 30 years and have become household words because the names are frequently mentioned in the media. But the database suggest otherwise. The GTD allows to identify more than 2000 separate terrorist groups that have operated somewhere in the

world from 1970 to 2011. One way to gauge how long a group lasts, is by looking at the time between their first attack and their last known attack. If the last known attack has not taken place in many years one can safely assume that, they've gone out of business. Using such data, one finds that nearly 75% of the terrorists organizations identified in the GTD, have lasted for less than a year. In general terms, terrorist organizations are somewhat like business startups, and likely to disappear in the first year of existence. Forming and maintaining terrorist organizations is not easy, despite impressions one might get from the media.



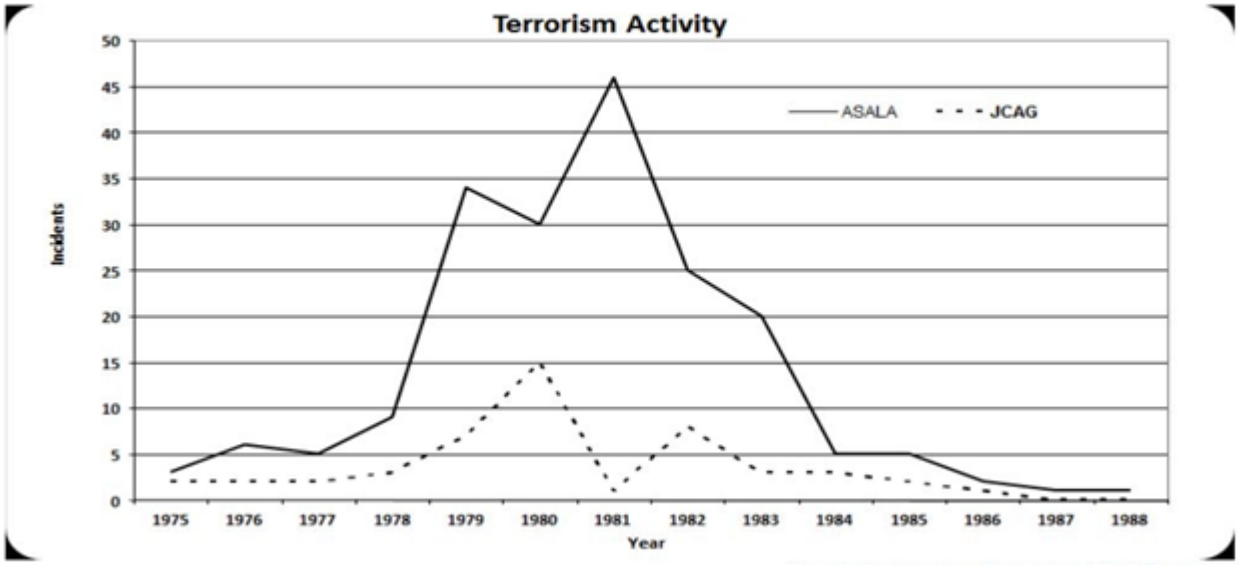
Why does society have the impression that terrorist groups are long lasting and difficult to eradicate even when the evidence does not suggest this is the case? The reason for this is that because the level of attention given to the ones most frequently mentioned the Al-Qaedas, the LeT, the ISIS', people assume that all terrorist organizations are around for a long time. But for every infamous household name, there are many more short lived and relatively unknown groups that people may never hear about. For example, groups like the Anti-Capitalist Brigades and the Revolutionary Flames, which one man or may not have heard of.

9. Finally, myth number nine, **terrorist groups are impervious to governmental counter terrorist policies and that they rarely make mistakes.** One could call this the myth of the super terrorist. Again, it follows dramatically from big, black swan, events like 26/11 and 9/11. Events seem very difficult, like one could not bargain a way out, and very impervious to be able to contain. So one gets this idea of their incredible advanced planning, destructiveness, and this contributes to the notion of these terrorists groups being somehow unstoppable and infallible.

When engaged in a number of research projects, which suggest that terrorists groups are not infallible, and they frequently make mistakes. Offer one example of a group called The Armenian Secret Army for the Liberation of Armenia, ASALA. It was a very active group, especially in the 1970s and 1980s, which was based in Turkey. After mounting a long series of deadly terrorist attacks throughout the 70s and 1980s, ASALA disappeared rapidly. Why did a group that was so

destructive and causing so much trouble disappear fairly rapidly? After studying different explanations and some statistical modelling of other researchers, a convincing explanation for the rapid decline of ASALA was their strategic shift.

Attacks by ASALA and JCAG, 1975 to 1988



Source: Dugan, Huang, LaFree and McCauley (2009)

Rather a strategic error in their targeting. Before the early 1980s, ASALA was careful to target Turks and to avoid non-Turkish, especially Armenians, as casualties or fatalities. This was important because Armenian support groups in ASALA were reaching out to the Armenian diaspora around the world. They also had quite a bit of sympathy from Western Europe, where many people saw them as having a reasonably just cause. But starting in the early 1980s they became less discriminant in their targeting methods. Started killing non-Turks and innocent people more frequently. The event that best represents the error was an attack at Orly airport in Paris, 1983. An explosive device detonated prematurely in the terminal area by the Turkish airline counter, it killed 8 people it wounded over 50. Many of the people who were killed and wounded were Non-Turkish citizens, include many from Western European countries. The increasing reliance on brutal random act of violence such as this attack polarized former supporters and created hostile climate within ASALA. It became difficult for ASALA to reach out and ask for financial support from the diaspora community around the world. ASALA seriously miscalculated the impact of their changing strategy on their supporters, and the sympathy of the Western Europe. This is not an isolated example, there are plenty of examples of misjudgment and even outright incompetence on the part of terrorists. So the super terrorists are not totally infallible.

Another example. Less than 90 minutes after detonating a massive truck bomb in front of the Alfred P Murrah Federal building in Oklahoma City in 1995, Timothy McVeigh was arrested for

driving without a license plate. You might think that you would've gotten your license plate in order if you wanted to avoid detection after committing a major terrorist attack.

There's another interesting example in 1993, a group of Islamic extremists drove a rented bomb laden van into the underground parking garage of the World Trade Center Complex. They then used the timer to set the bomb to detonate, when the bomb exploded, it killed six people and wounded over a thousand more. It was kind of a shocking precursor actually to the 9/11 attack, but what's remarkable about this attack, is 3 hours after the explosion, one of the chief conspirators on the plot, Mohammed Salame Returned to the Ryder rental agency in New Jersey to get his deposit for the rented van back. It gets even more curious, when the rental company refused to return his $400 deposit without a police report, Salameh went to the police to report the van stolen. Eventually, Salameh's desperate attempts to get his $400 deposit back unraveled the entire conspiracy.

During 26/11, terrorists who came in their own boat from Pakistan, hijacked the boat of Indian fishermen midway. Used the hijacked boat to enter Indian waters. Terrorists prepared the inflatable boat on the deck of the hijacked boat after coming close to the coast of Mumbai. The inflatable boat was found abandoned on Mumbai coast, it had a Yamaha engine. The unique number on the engine had been erased by the conspirators. Yamaha shared the technique held secret by the company with India’s engineers, who were able to retrieve the number.

They found the engine number of the boat. The FBI sent one of its agents to the headquarters of Yamaha Motors in Japan to seek help in tracing the person who purchased the engine. The unique number on the engine had been erased by the conspirators, who had brought an inflatable boat form Pakistan. The engine was then traced to a Karachi shop which sold eight such engines to a chief financier of Lashkar-e-Taiba (LeT).

Conclusion

Contrary to our stereotypes based on 26/11 and a few other extraordinary black swan events. Considering a number of terrorist attacks in the past two decades, most of them have largely relied on readily available, unsophisticated weapons. The attacks frequently involve few or no fatalities, and a typical terrorist group disappears in less than a year. Very few attacks involved disgruntled groups from one country attacking civilians in another country. There is ample evidence that terrorists frequently make strategic errors. Attacks were declining just before 9/11, and rose until 26/11 before declining yet again. This article makes one think about terrorism from a social science standpoint, not just an individual high profile case studies, but makes one think about terrorism in a

much broader context. This helps us win, in the least terms, a perception war against the terrorist. Since it takes away at least one objective from the terrorists, and that is public attention.

References

Asal, Victor, and R. Karl Rethemeyer. "The nature of the beast: Organizational structures and the lethality of terrorist attacks." The Journal of Politics 70.2 (2008): 437-449.

Byman, Daniel. "Do targeted killings work." Foreign Aff. 85 (2006): 95.

Crenshaw, Martha. "Theories of terrorism: Instrumental and organizational approaches." The Journal of strategic studies 10.4 (1987): 13-31.

Cronin, Audrey Kurth. "ISIS is not a terrorist group: Why counterterrorism won't stop the latest jihadist threat." Foreign Aff. 94 (2015): 87.

Ganor, Boaz. "Terrorism as a strategy of psychological warfare." Journal of aggression, maltreatment & trauma 9.1-2 (2005): 33-43.

Giddens, Anthony. Runaway world: How globalization is reshaping our lives. Taylor & Francis, 2003.

“Global Terrorism Database,” University of Maryland, https://www.start.umd.edu/gtd/ Accessed 18th July 2019.

“Global Terrorism Index,” Institute for Economics and Peace, http://visionofhumanity.org/app/uploads/2018/12/Global-Terrorism-Index-2018.pdf Accessed on 20th July 2019.

Goodwin, Jeff. "A theory of categorical terrorism." Social Forces 84.4 (2006): 2027-2046. Held, Virginia. "Terrorism and war." The Journal of Ethics 8.1 (2004): 59-75.
Jenkins, Brian M. International terrorism: The other world war. No. RAND/R-3302-AF. Rand Corp Santa Monica CA, 1985.

Jenkins, Brian Michael. "The new age of terrorism." The McGraw-Hill homeland security handbook (2006): 117-130.

Jongman, Albert J. Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature. Routledge, 2017.

Khetan, Ashish, et al. 26/11 Mumbai Attacked. Roli Books Private Limited, 2009.

Krueger, Alan B., and David D. Laitin. "Kto kogo?: A cross-country study of the origins and targets of terrorism." Terrorism, economic development, and political openness (2008): 148-173.

LaFree, Gary, and Laura Dugan. "Tracking global terrorism trends, 1970–2004." To protect and to serve. Springer, New York, NY, 2009. 43-80.

LaFree, Gary, and Laura Dugan. "Trends in Global Terrorism, 1970-2011." in Peace and Conflict: 2014. Routledge, 2017. 39-52.

LaFree, Gary, Laura Dugan, and Erin Miller. Putting terrorism in context: Lessons from the Global Terrorism Database. Routledge, 2014.

LaFree, Gary. "Countering Myths about Terrorism: Some Lessons Learned from the Global." What Do We Expect from Our Government 71 (2012).

LaFree, Gary. "The global terrorism database (GTD) accomplishments and challenges." Perspectives on Terrorism 4.1 (2010): 24-46.

LaFree, Gary. Using open source data to counter common myths about terrorism. Cambridge: Cambridge University Press, 2011.

Mir, Amir. Talibanisation of Pakistan from 9/11 to 26/11 and beyond. Pentagon Press, 2010.
Ragavan, Chitra. "Tracing terror's roots." US News & World Report 2003 (2003).
Rosenfeld, Richard. "Terrorism and criminology." Terrorism and Counter-Terrorism. Emerald Group Publishing Limited, 2004. 19-32.

Sanderson, Thomas M. "Transnational terror and organized crime: blurring the lines." SAIS Review of International Affairs 24.1 (2004): 49-61.

Silke, Andrew. "Research on terrorism." Terrorism informatics. Springer, Boston, MA, 2008. 27-50.

Taleb, Nassim Nicholas. The black swan: The impact of the highly improbable. Vol. 2. Random House, 2007.

Tilly, Charles. "Terror, terrorism, terrorists." Sociological theory 22.1 (2004): 5-13.

Industry 4.0: What does it mean to Military?

Wing Commander Jayesh C S Pai (Retd.)
Commandant,
Bhonsala Military School
Email: jcspai@gmail.com

Industry 4.0 refers to the fourth industrial revolution – an incoming era of cyber-physical systems powered by artificial intelligence (AI), the Internet of Things (IoT), autonomous machines, and big data. It is the next evolutionary step up from our current digital revolution into a new age of connected technologies and data-driven insights.

Certainly, i4.0 promises big things for manufacturers across all industries. That includes the defence sector where advanced manufacturers in the commercial and military space are being propelled forward to produce autonomous systems, robotics and augmented reality solutions for land, sea, air, and space environments.

As a result, business is beginning to see the promised cost-saving benefits and performance improvements that come with removing the man from the production machine. As more manufacturers invest in smart, connected, and self-maintaining equipment, we can expect the cost of ownership to shrink and the barriers to market entry begin to erode.

These technologies go hand-in-hand with advancements in data analytics, cloud computing, and artificial intelligence. With these pillars of i4.0, manufacturers will have the means to more accurately predict and respond to any Defence Force supply needs, achieve smarter resource management, and use chips and sensors to better track and manage inventory and other assets. Ultimately, investments in the digital supply chain elements of i4.0 will improve speed to market, lower production costs, and facilitate more collaborative innovation. And considering that a significant share of aerospace and defence products is supplier developed, it is investments like these that will prove to be critical enablers for industry and military leaders alike.

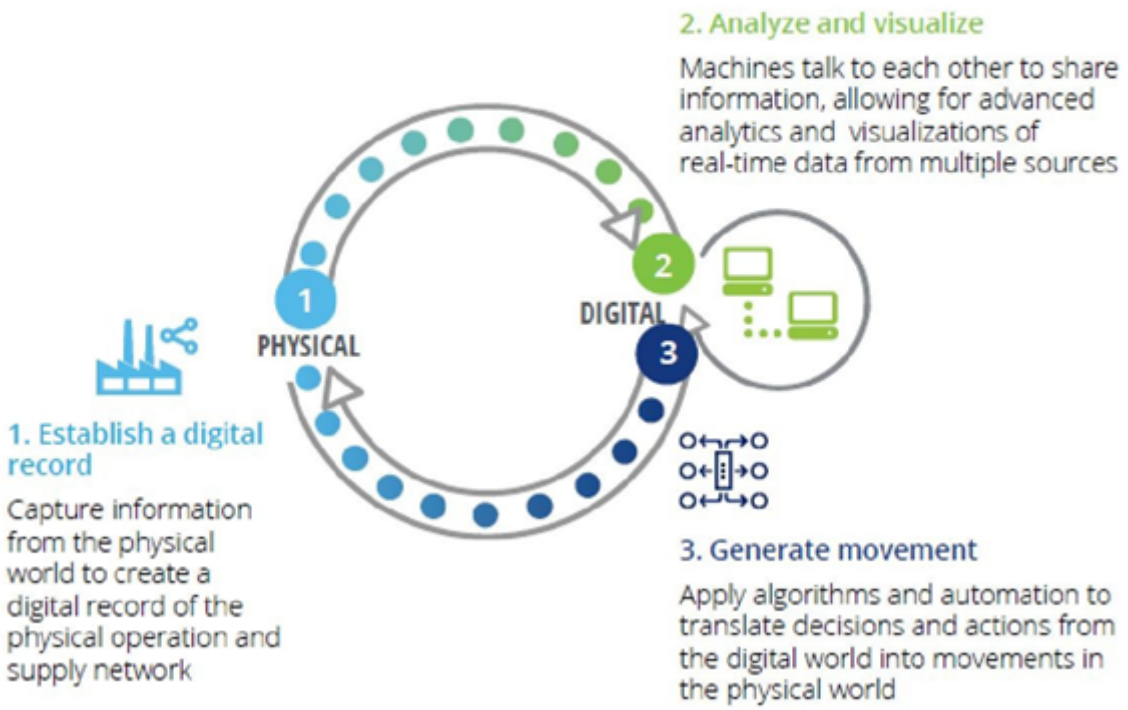
What is Industry 4.0?

The concept of Industry 4.0 extends digital connectivity into the physical world. Industry 4.0 technologies combine digital information from many different physical and digital sources and locations, including theInternet of Things (IoT) and analytics, additive manufacturing, robotics, high-performance computing, artificial intelligence and cognitive technologies, advanced materials,

and augmented reality. These data sources come together to improve operations in an ongoing cycle known as the physical-to-digital-to-physical (PDP) loop (figure 1).

FIGURE 1

The Industry 4.0 physical-digital-physical loop



Throughout this cycle, real-time access to data and intelligence is driven by the continuous and cyclical flow of information and actions between the physical and digital worlds. Many organizations already have some portions of the PDP loop in place, namely, the physical-to-digital (sensors providing data about key assets), and digital-to-digital (digital analytics tools) processes. However, it is the leap from digital back to physical—from connected, digital technologies to action in the physical world—that constitutes the essence of Industry 4.0.

Industry 4.0 In The Real World: Machine Learning In Supply Chains

Restaurants may seem like a familiar, simple business, but many feature complex supply chains with planning and actions reminiscent of military operations. Ingredients must be delivered regularly so that they are fresh, but all of that depends on the rate of use, which depends on how often customers order different dishes—something outside the control of the restaurant. Traditionally, this was done manually by tallying up how much of each ingredient had been used and guessing when it would need to be reordered. This could lead to over-ordering and waste, or ordering too late and not being able to fulfill customers' orders.

One restaurant chain decided that there was a better way to manage its supply chain. The restaurant chain used machine learning and AI tools to analyze point-of-sale data. Soon, the system was able to "learn" how much of each ingredient was used for each type of order. Rather than forcing planners to predict based on the information they had on hand at the moment, the restaurant chain used a seamless flow of real-time data to begin to sense, anticipate, and even forecast demand. This improved forecast accuracy by 25 percent, reduced the workload on staff, and achieved a 99 percent in-stock rate for each restaurant. Even more importantly, the benefits cascaded down the supply chain, with every supplier being able to better plan. The result was less waste, timelier deliveries and the right dish on the customer's plate—every time.

Better knowledge, better predictions, and better performance: a lesson equally applicable in the restaurant as it is to the military. In fact, the US Navy is using similar machine learning tools to prioritize and route the huge volumes of message traffic that ships and submarines receive.

Industry 4.0 In The Real World: Iot And Predictive Maintenance

The challenge with traditional maintenance strategies is that it can be difficult to predict what will happen with a given machine. Therefore, companies typically must stock a wide variety of different spares to be prepared for any failure. However, IoT-based sensors and predictive maintenance algorithms can offer a more efficient solution by providing insight into the condition and status inside each piece of machinery. Italian train operator Trinitarian was looking for exactly such a solution when it faced performance penalties for schedule delays created by unexpected maintenance on its trains. To address the problem, Trenitalia added hundreds of on-board sensors on 1,500 locomotives. Data from those sensors was then transmitted to private cloud storage in near-real time, where diagnostic analytics provided advance warning of the failure of parts such as brake pads. With such data, Trenitalia was able to maximize the brake pads' useful life while reducing unexpected failures. With these sensors and predictive maintenance algorithms, Trenitalia were able to decrease downtime by 5–8 percent and reduce its annual maintenance spends by an estimated 8–10 percent, saving about $100 million per year.

While the maintenance demands of a commercial business with relatively predictable schedules are different than the hard-wearing, anytime, anywhere demands on military platforms, the same predictive maintenance techniques are already being used by some militaries around the globe. For example, the US Army is using predictive maintenance on a portion of its fleet of Stryker combat vehicles using more than 5 billion data points from on-board sensors.

Industry 4.0 In The Real World: Digital Twin

The collection of data and technologies is what the industry would call a "digital twin." A digital twin is an evolving digital profile of a physical object or process that helps optimize business performance. Digital twins start with complex models of the object or process they wish to mirror and then update them over time with data streaming from the real-world thing as it operates. The digital twin can mirror a physical object such as a particular jet engine or an entire process such as what is happening on a factory floor. Most importantly, these twins are not just for show but can be tested in ways that their physical counterparts cannot. For example, Formula 1 racing teams have digital twins of both their cars and the tracks they race on. They use these twins to run complex simulations of race strategies, often with the drivers in the car, so that on race day, they know exactly what tires to use, when to stop, and all the other settings that will give them the best chance of a win. Just like race teams, the military has long sought to prepare for the future with war-gaming and simulation. However, the ability to make those simulations more accurate via the use of a digital twin is a game changer and can produce a more lethal force at a lower cost than ever before thought possible.

Getting to "Know"

A new approach to readiness based on real world data may seem almost impossible to implement. After all, finding the location and status of every piece of equipment and every service member seems a nearly insurmountable challenge. However, this large task can be made simpler by breaking it up into smaller and more manageable problems where existing solutions can help. In fact, portions of such a solution are already at work in many commercial companies using Industry4.0. The core of Industry 4.0 involves using digital information about the physical world to improve decisions and actions taken in the physical world.

With more accurate information about the physical world, organizations can make better decisions, faster. No company faces the same daily challenges as the military, so merely importing solutions wholesale from the commercial world will never work. However, the core issue of readiness is similar in nature to the business challenges faced by many companies. Therefore, the approaches and technologies of industry, when recombined in new ways, can help to solve similar challenges for the military.

In this way, manufacturing company struggling with efficiency could look very much like a military organization struggling to determine its readiness. Both need to know the location of their assets, the condition of key components, and whether the current status of equipment can meet the

current demand from orders. To put that in terms of the three readiness questions, both militaries and companies need to know the need, know the assets, and know the best action to take. For the military, this means that the three questions of readiness each require information of a certain type:

- What capabilities are needed for expected missions requires that we know the need, which means correlating mission parameters to the force requirements and capabilities needed to execute.
- What is the status of those capabilities requires that we know the assets, meaning a real-time, on-the-ground picture of the status of the Joint Force down to the individual tank, aircraft, and service member.
- How to allocate the next rupee to improve those capabilities requires that we combine those data streams so that leaders can know the best action. Correlating force requirements for likely missions with the real-time picture of available people, systems, and infrastructure allows leaders to understand where shortfalls may exist and where additional funding could be most effective.

Know the need

Knowing what capabilities are needed for a mission may seem to be the simplest of all readiness issues for the military. After all, the units and capabilities needed for key missions are typically set out long in advance in strategic plans at every level of command. But there can be large difference between military operations as planned and military operations as successfully executed. After all, as the old adage goes, “No plan survives first contact.” Therefore, to truly understand how ready a force is to execute a mission, militaries should not only look at what the plan calls for but also what has been done in the past in real-world missions. This is much more than just looking at the order of battle or lists of units. Rather, it is about understanding how different parameters of a mission place demands on the forces that will execute that mission. Everything from the task, to the terrain, to the weather, to the particular enemy being faced can change the makeup and skills needed to execute that mission. Operating at high altitude? You will need more helicopters due to reduced load in the thin air. Tasked with a foreign internal defence mission? You will need junior personnel with local language skills. The huge variety of different factors makes predicting future force requirements exceedingly difficult. Here, machine learning can step in to provide an answer and ease the workload. Today, machine learning is all around us performing tasks from recognizing hand-written digits to recognizing patterns of credit card fraud. A machine learning tool using neural networks or another approach can be trained to associate the

various mission parameters (e.g. task, enemy size, terrain, weather, time, and so on) with the size and capabilities of the force needed to accomplish them. Over time, the neural network will become trained enough to anticipate the need for wholly new mission parameters it has never seen before. In other words, the machine learning tool will be able to reliably suggest the required capabilities for future missions. But most importantly, these suggestions will not be based on assumptions or best guesses; they will be based on hard-won lessons from real-world missions.

Know the assets

While a complete picture of real-world mission needs can ease planning, the right capabilities still need to be available to carry out those plans. This challenge goes far beyond any patch chart or doctrinal table of organization. It gets at the heart of the factors that make military units successful. Some of those, like having the right equipment, are easy to see and measure, while others, like having local knowledge or experienced leadership, can be more difficult to observe. A real-world, real-time picture of the location and status of personnel, equipment, and infrastructure down to the individual level can help address this challenge. After all, it doesn't matter if a unit is designated with a regional specialty in West Africa; it matters if the squad leader can speak French. In fact, this more granular picture of capabilities can supercharge the benefits from task organization that the military already enjoys. Today, task organization tends to exist only at the unit level, blending different units with different capabilities to create a task force tailored to a mission. However, with a more granular picture of the equipment, personnel, and infrastructure, commanders could combine individuals with the right skills and experience with equipment in the right place at the right time to create more capable formations in shorter time. Rather than just seeing red or green stoplight charts, a commander could see that a helicopter may not be ready for its squadron's upcoming combat deployment due to inoperable radar warning system, but could support disaster relief mission with a different unit.

Similarly, an individual soldier may seem "non deployable" due to upcoming paternity leave, but a more detailed picture of his skills and availability may show that his language skills may make him an ideal fit for a short-term deployment to support a foreign exercise.

Know the best action

With a real-world picture of mission needs and a real-time picture of available capabilities, militaries can evaluate their preparedness in detail, potentially for the first time. But that is not the end of the story. Even more important is the question of how to improve that preparedness. When

there is inevitably a gap between required and available capabilities, planners need to know where future investments should be directed to remedy that gap. Is the problem a lack of specially certified personnel, a shortage in a type of aircraft, or even a need to have more qualified units in an insertion technique? What is typically needed is some sort of enterprise decision support capability. Luckily, machine learning techniques can again be applied here to answer those questions and ultimately ensure that the joint force is more capable, lethal, and affordable than before. By combining the real-world and real-time pictures of force capabilities, planners can create what is essentially a "digital twin" of the force. This digital, data-driven picture of the force allows leaders to conduct detailed scenario planning. They can test the force against different types of missions and combinations of missions in ways that would be impossible to recreate in real life. Moreover, by seeing how the force stacks up against these various mission requirements, planners can understand where gaps in capability exist and where the next dollar of investment should be spent to best fill those capability gaps—whether through additional capacity, greater training, or new material.

Membership Details

Membership

- Patron Member
- Life Member
  - A person who donates a minimum of Rs. 10,000/- is entitled to become a life member.
- Students Member
  - Any Students enrolled for any courses in statutory University or establishment can apply for such membership by paying or ending Rs.1000/- for one academic year. Any Student member can't step up to the category of Donor member by fulfilling the terms & conditions given for the Donor Member.

Note :-

- Acceptance of becoming a member of each category will be subject to the approval of the executive committee
- Members will be provided information and facility to different activities undertaken by the centre.
- Library facility will also be provided to the member of each category as per procedure prescribed by the Director.

Advertisement (Per Issue)

Sr. No.	Particulars	Per Issue
01	Back Cover Page	Rs.15000
02	Inside Cover Page	Rs.10,000
03	Full Page	Rs.5,000
04	Half Page	Rs.2,500
05	One Fourth Page	Rs.1,000

Membership (Daksh)

Sr. No.	Particulars	Per Issue
01	Institution (Life Membership)	Rs.25,000
02	Individual (Life Membership)	Rs.15,000
03	Students for 3 Yrs.	Rs. 2,500
04	Students for 2 Yrs.	Rs.1,500
05	Students for 1 Yrs.	Rs.1,000
06	General Membership (Yrly)	Rs.1500

Bhonsala Research Centre for Conflict & Peace

Bhonsala Military College, Nashik-422005

Membership Card

Name : _____

Address : _____

_____

I/We wish to become a member of BRCPP as Patron / Institutional / Life / Student please find herewith membership free of Rs._____ by Demand Draft/ RTGS/ Cash

Signature_____

For Office Use Only

Details of Payment

Bank/ Cash/ :-_____

Drawn on:-_____

Date:-_____No.:-_____

Amount Rs.:-_____

Sign of A/c clerk

Note:

Draft / RTGS/ Cash to be made favouring Principal, Bhonsala Military College, Nashik (Postal Order will not be entertained)

Resolution No._____ Passed by the Committee Meeting of _____	For BRCCP Office Membership :-_____ Nature :-_____ No :-_____ Sign of Co-Ordinator

Communication Details

Name of College	:-	Bhonsala Military College
Postal Address	:-	Rambhoomi, Dr.Moonje Path, Nashik-422005, Maharashtra, India
Website	:-	www.bmc.bhonsala.in
E-Mail	:-	principal@bmc.bhonsala.in
Phone No	:-	0253-2309610 / 12 / 13
Fax No.	:-	0253-2309611

For Contributors

Name of Chief Editor	:-	Dr.P.A.Ghosh
Address	:-	Room No. 44, 1st Floor, Department of Defence & Strategic Studies Bhonsala Military College Camps, Rambhoomi, Dr.Moonje Path, Nashik-422005, Maharashtra, India
Email	:-	drpaghosh@gmail.com
Email	:-	daksh@bmc.bhonsala.in
Phone No	:-	0253-2309610 / 12 / 13 (Ext:-228)
Mobile No.	:-	+91-9421605171

Dear reader,

Consider this as a personal letter to you, yes you in particular, I would like to introduce you to a person whom I did not know a few years back but who has now become a part of my daily routine. He is slightly taller by today's standard, his feet firmly founded on the ground as he stands tall. Exceptionally well groomed for a seventy five old. A side parted wavy sweep-back hair with movement. Whenever he is out and about he wears a classic headgear, round black cap that stands three inch above the crown. On auspicious occasions he would wear a traditional turban.

Pensive eyebrows, thick and dark, with a peanut shaped religious mark (tilak) between them. Visibly wet and piercing eyes, like it has witnessed the depth of the sea, the height of the mountain, and everything in between. I see brown mountainous pupil and iris with a hint of a sea green colour, his eyes depicts the whole Indian Peninsula.

Being an ophthalmologist, he has set his sight very firmly on a goal, as reflected by the determination of his spectacles to rest on his pride - the nose. The weight of all the social commitments has a rightful estate on this very nose. His spectacles is round, bifocal and with a golden frame. The distant vision is to breathe the promised aroma of thriving sustainable Swadeshi economy that comes with Swarajya (self governed) and it is guided by Swadharma. This self sufficiency could be achieved by the near (immediate) vision lens of his bifocal eyepiece, the competence of an indigenous military men.

Imagine a combination of Scimitar skyrim & maratha talwar (sword), now mirror your imagination to visualise his sharp and rigid silver mustache. A centrifugally groomed 'taking charge' beard, the length extends to hide his collar bone. The contemporary name for this silver fox undercut beard style is 'Bandholz'. Underneath is a wrinkle free long coat, knee length, combined with regular fit pajama and black mojari shoes.

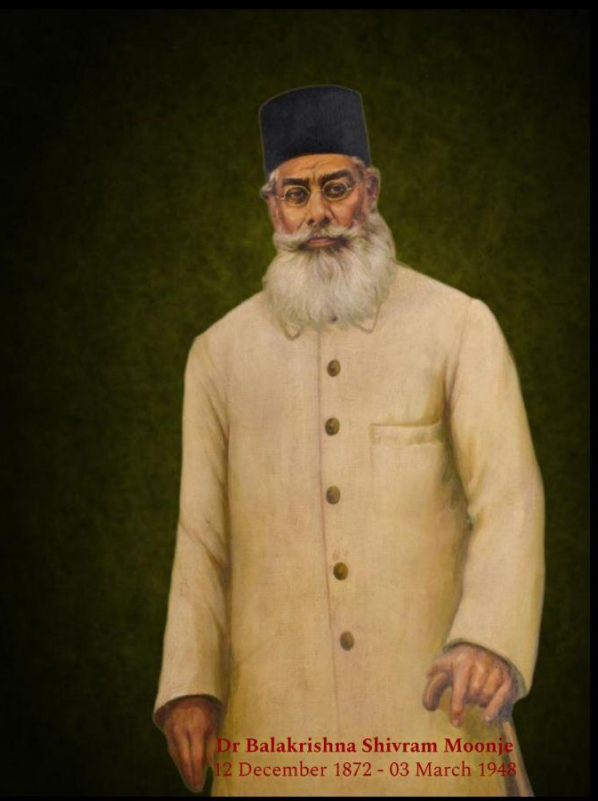
He carries a stout danda in ever youthful spirit and has a deep baritone voice. A luminous personality with robust military attitude, who can work his magic from the pen, the gun and the forceps alike.

Life presents us with people from the past, we must learn, cherish and treasure them. We never know where the future will lead us but we certainly know where we come from, I think that is enough to shape our today with.

Dear readers, with DAKSH we hope to pay a fitting tribute to Dr B. S. Moonje who laid the foundation of Bhonsala Military Campus and called it Rambhoomi. The Sthitapradnya Head of Bhonsala Family and Guardian to our Ramdandee trainees/students. A person whom we owe a great debt. He lived to create the future we live in today.

May we have the ability to empower the nation he foresaw - with the best of what we have, for the best that can be.

from a bearer of
the Danda of Shree Ramchandra,
Your Ramdandee



Dr Balakrishna Shivram Moonje
12 December 1872 - 03 March 1948


अग्रतश्चतुरो वेदाः पृष्ठतः सशरं धनुः। इदं ब्राह्ममिदं क्षात्रं शापादपि शरादपि।।