idsa
INSTITUTE FOR DEFENCE STUDIES & ANALYSES
रक्षा अध्ययन एवं विश्लेषण संस्थान

Role of Technology in International Affairs

Amitav Mallik

ROLE OF TECHNOLOGY
IN
INTERNATIONAL AFFAIRS

ROLE OF TECHNOLOGY IN INTERNATIONAL AFFAIRS

Amitav Mallik

INSTITUTE FOR DEFENCE STUDIES & ANALYSES
NEW DELHI

PENTAGON PRESS

Role of Technology in International Affairs

Amitav Mallik

First Published in 2016

ISBN 978-81-8274-881-1

Published by

PENTAGON PRESS
206, Peacock Lane, Shahpur Jat,
New Delhi-110049
Phones: 011-64706243, 26491568
Telefax: 011-26490600
email: rajan@pentagonpress.in
website: www.pentagonpress.in

Branch
Flat No.213, Athena-2,
Clover Acropolis,
Viman Nagar,
Pune-411014
Email: pentagonpresspune@gmail.com

In association with
Institute for Defence Studies and Analyses
No. 1, Development Enclave,
New Delhi-110010
Phone: +91-11-26717983
Website: www.idsa.in

Printed at Avantika Printers Private Limited.

Contents

Preface

In international affairs diplomacy, technology and economics are the most important tools for any nation. Historically, science and technology (S&T) has been one of the main currencies for exchange and dialogue among human societies and sovereign nations. In modern times, it is emerging as an important instrument of techno-economic power that will shape the changing dynamics of international relations and global affairs. Diplomacy is the major instrument of dialogue between nations. It is the art to negotiate to protect one's interests and promote one's influence in international affairs. For every sovereign nation both technology and diplomacy are essential tools for managing international relations, the essence of which is protecting national security and projecting national power.

Throughout history of international affairs, S&T has been a defining factor in the evolution of security and war-fighting strategies among nations. These strategies have depended largely on the level of technology available to warriors and leaders. Today, technology has multiplied the human capacity to cause damage or destruction and hence, diplomacy has an enhanced role in preserving peace. As sovereign nations struggle to gain better position vis-à-vis other nations, with or without open conflict, the competing forces often get translated into 'threats', with more powerful parties often gaining the advantage. These are the advanced nations which define the global norms and set standards for others to follow, who often aspire for similar powers through indigenous techno-economic progress or by forming alliances to achieve their aims. Others, who cannot keep pace with the powerful, often become rebellious and seek certain nuisance value to climb up the ladder. In such dynamics, whether at the national or international level, it is the techno-economic capability and diplomatic-military strategy that provide the real vital edge to a nation. Thus, in international affairs, technology and diplomacy will have to play the final defining role for every nation.

S&T has played a key role in creating the globally connected modern societies of today. While automobile and aviation technology brought about revolutionary changes in speed and time of travel, electronics and communication technology created whole new capabilities in information and communication exchange. Advances in S&T have been driven by man's aspiration for progress and peace. His innovative instincts and experimental skills have evolved with his pursuit of a secure environment, economic prosperity and defence from threats to his sense of well-being. As witnessed in the 19th and 20th centuries, advances in S&T have proved to be powerful drivers of change in global society as well as among nations in terms of economic, military, political and even cultural development. S&T has been so intrinsic to the process that it is often taken for granted and seldom recognised for its important independent identity and its intrinsic role in policy formulation, both at national as well as global levels.

Of course, the progress among societies or nations using S&T with innovative imagination has not been equal and this has created significant inequality among nations; such that faster developing societies have acquired relative superiority over other slower developing societies. This has led to the need for protecting individual national assets and interests from competitors and adversaries. The resultant techno-economic divide has been growing since the industrial revolution. Technological superiority, combined with man's ideology and ambition for power and control thus underscores the basic dynamics of interactions amongst societies and this indeed has become the very rationale for international relations and diplomacy.

Advances in S&T have been used with great success for multiplying man's defensive and offensive powers beyond local horizons. Technology has created lethal weapons of war and even weapons of mass destruction (WMD), albeit supposedly to provide the ultimate deterrence to war, so as to maintain peace. The cold war between the two superpowers for over 40 years was marked by relentless pursuit of S&T for maintaining the techno-military edge over the adversary. This in effect produced accelerated development of advanced technologies that shaped the political and military doctrines as well as the methods and means of waging war or preserving peace. Information technology has emerged as the backbone of the present 'Knowledge Society'.

In the modern world of today, technology is so intimately embedded in national priorities and international equations that it has become an inseparable component of international relations and diplomacy. This book hopes to highlight this important relationship and discuss the increasing role of S&T in international affairs.

The role of S&T in the present 21st century is far more relevant and yet its interplay in international affairs is almost invisible in the globalised society. In fact, much of the globalisation and consequent inter-dependency among societies and nations is because of the integration brought about by advances in Information-Communication-Technology (ICT). Technology has enabled modern civilisation to move towards a knowledge-based society where the information flow is instantaneous - far improved compared to a decade ago. More recently, S&T has been effectively used by nations for soft-power projections. In this changing paradigm, it is highly desirable to understand the importance of S&T dimensions of international relations and the changing dynamics of diplomacy among nations.

Unfortunately, S&T advances have also led to unintended consequences of phenomenally high rates of development particularly in the past five decades, which have led to rapid depletion of earth's resources and accelerated global warming with associated loss of biodiversity that will affect the future of human societies. Shortages of resources and concerns of environment are fast becoming one of the more serious global concerns that cannot be addressed without major interventions using both S&T as well as diplomacy for constructive and lasting international cooperation. Thus, the major challenge for 21st century diplomacy will be to prevent misuse of technology from harming mankind and environment.

The book endeavours to highlight the increasing role that modern technology is bound to play in international relations and global affairs in the future. It is hoped that the book will succeed in bringing a renewed focus on the importance of S&T integration with foreign policy and indeed with overall national aspirations, particularly for India.

Amitav Mallik

Acknowledgements

As a defence technologist, I have been very fortunate to get the opportunity to create the office of 'Adviser, Defence Technology' at the Embassy of India, Washington DC and serve there for six years during the most challenging time for Indo-US technology cooperation. This gave me first-hand experience on how technologists and diplomats can combine strengths to serve the foreign policy objectives of the nation.

I was yet again fortunate to serve as a Member of the National Security Advisory Board for three consecutive years immediately after my retirement, and this gave me the opportunity to acquire a wider understanding of the interplay between technology, foreign policy and national security. Then to get an opportunity to use my experience and knowledge to write a book on 'Technology and International Relations' is like a dream come true for me. For this, I am indebted to DG, IDSA for giving me this opportunity.

The topic for the book was actually suggested by Dr. Arvind Gupta, DG, IDSA in 2012 and while conceptualising the book I have gained immensely from discussions with several of my advisers and friends like Dr. Arvind Gupta, Ambassador Arundhati Ghose, Dr. Ajey Lele, Mr. Kapil Patil and many others. I owe them all very sincere thanks.

While researching for the book I took help from three promising research assistants – Mr. Harshad Garje, MSc, Defence Studies, Pune University; Ms. Meenu Raina MSc, Environmental Sciences, Pune University and Ms. Sonal Jain, BSc (Hons), Political Science, Miranda House, Delhi. The research support they provided was excellent and I want to thank them very sincerely and wish them all the very best in their future professional careers.

I must thank the IDSA Library staff and administration for providing ready support from time to time and a special thanks to Ms. Sumita Kumar who provided the coordination support and very substantial editorial help.

Last but not the least I must thank my life partner Surbhi, who despite being very unwell during most of 2013, happily adjusted to my pre-occupation with the book project which must have caused some inconvenience at home.

Amitav Mallik

PART I

Role of Science and Technology in International Affairs

1

Technology, Diplomacy and International Affairs

Introduction

The decades of cold war between the United States (US) and the erstwhile Union of Soviet Socialist Republics (USSR) demonstrated beyond doubt how science and technology (S&T) could be leveraged actively, not only for avoiding war but also in the conduct of 'International Relations' (I.R.) to maintain diplomatic balance. The game changing technology of nuclear weapons (NW) is often credited with bringing World War II to an abrupt end, saving continued destruction and loss of life. More recently, the technological race between the two superpowers in which the US managed to gain a decisive techno-military edge by 1990, is also perceived as the major catalyst of the Soviet economic impoverishment that eventually led to the fall of the Soviet 'empire' without any armed engagement or war. Few could have anticipated that technology would finally provide a solution for ending the cold war that could have caused mutually assured destruction.

The very concept of 'Deterrence' via techno-military supremacy over the adversary is nothing but coercive diplomacy using the advantage of technological superiority. Technology denial regimes are classic examples of 'Science Diplomacy' being exercised to serve the foreign policy agenda of powerful nations. The international focus on non-proliferation of NW can be viewed as a discriminatory technology-control measure against specific

countries. It is interesting to note that during the cold war decades, there was also effective use of science diplomacy to reduce tensions and enable confidence building measures (CBMs) despite the existence of great strategic rivalry and mistrust. Thus, there is ample historical evidence that S&T has been in extensive use not only for waging battles or winning wars but also for creating conditions suitable for preserving peace. Technology per say is not good or bad; but how it is used by the user determines the impact.

In recent decades since the end of the cold war, economic globalisation and explosive growth of Information-Communication-Technology (ICT) has dominated the political and corporate agenda that is defining a new paradigm where competition and cooperation must coexist amongst most pragmatic societies and nations. This will call for skilful diplomatic manoeuvring of different priorities in future that will have to be based on sound understanding of the role of S&T in international affairs. Our world is far more interconnected today, where no nation can afford to be isolated, no matter how powerful or self-sufficient. Technologies of global reach are changing the reference lines and timelines of the geopolitics of international interactions, diplomatic perceptions and global affairs.

The competition for techno-economic power has become increasingly serious among nations and there is clear realisation of the impact of technology on economic progress, military might as well as on statecraft that shapes the balance of power equations among nations. Technology will continue to be one of most sought after commodities in international affairs.

While everyone agrees that military-economic strength will dictate future power equations among nations, there is unfortunately not enough understanding about the role that technology plays in this regard. It is often said that scientific research creates knowledge and innovation converts knowledge into economic wealth. Hence, it is worth noting that technology advances of the past few decades have been instrumental in creating globalisation which is essentially a socio-economic phenomenon. But this has also caused a paradigm shift in security perceptions and altered the techno-military doctrines of powerful nations. Enabling technologies such as advanced computing, ICT, bio-technology and nano-technology are transforming the spectrum of civilian as well as military applications. Today, most critical technologies for defence are increasingly for dual purposes, with civilian technology advances often feeding many military requirements and vice-versa.

Diffusion of technology has become an integral component of

international techno-economic transactions. Advances in sensors, smart materials, missile guidance, outer space systems, energy beam weapons and cyber space technology etc. are leading to new capabilities for offence and defence. Consequently, preventing misuse of advanced technology is much more challenging. While technology controls will remain important in I.R., new approaches to enable S&T cooperation among progressive nations will also be vital for the future. The private sector is increasingly becoming the main player in international technology exchanges while the role of government agencies is changing to being more a facilitator than controller. Developing nations in need of technology may face complex challenges of new criteria for technology transfer based on assurance of responsible ownership and use of sensitive technology. Such emerging trends will pose new diplomatic challenges to the demand side as well as the supply side of international exchanges.

The techno-economic progress of large sections of the growing world population is increasing the global consumption of energy and other earth resources at an alarming rate. This is amplifying the ecological footprint of mankind in ways that is altering the chemical, physical and biological makeup of the earth on a geological scale. It is becoming increasingly clear that this modern way of life will not be sustainable in the future and hence there is urgent need for coherent and well-coordinated international cooperation to moderate global consumption and its adverse impact on earth environment. S&T is the common denominator for all interactions and hence modern diplomacy, for effective international negotiations for global solutions, must recognise the vital role of S&T in international relations.

It can be argued that to develop a better understanding of transformation in global affairs, technology has to be integrated more synergistically into the theoretical discussions of I.R. Technology should be understood as a highly political entity and an integral core component of the global system that shapes global affairs and is itself shaped by global economics, politics, and culture. Foreign policies of nations and international equations in future will be enriched by a clear understanding of how technology and the global eco-systems interact with geopolitics and how global politics, economics, and culture impact technological evolution.

Global problems and concerns will require global solutions and will have essential diplomatic dimensions. The primary objective of science diplomacy is to support foreign policy objectives with scientific information and advisory. While this facilitates smoother international relations, it can also help to

improve S&T cooperation. Combination of S&T and diplomacy can thus provide soft power to countries for their international outreach objectives. Scientific exchange and technology cooperation can also contribute significantly to coalition building and conflict resolution, both vitally important to international peace. This chapter will focus on the above issues to highlight the role of S&T in international affairs.

Changing Dimensions of International Relations and Diplomacy

'International Relations' is the study of politics between States. Until recently, this largely meant the study of war and diplomacy but since the end of the cold war, the boundaries of I.R. have expanded to include trade, ethnic relations, human rights and many other topics that may cross State boundaries. The term 'science and technology diplomacy' is used to mean the provision of a science and technology advisory for multilateral negotiations and assessment of the results of such negotiations at the national level. It therefore, covers activities at both the international level and the national level, pursuant to international commitments. Today, in a globalised world, the core idea of I.R. is the interdependence and discourse between two or more key nations of the international system.

International relations can also be defined as a branch of political science, that studies foreign affairs and global issues among States within the international system, including the roles of States, inter-governmental organisations (IGOs), non-governmental organisations (NGOs), and multinational corporations (MNCs). It is both an academic and public policy field and can be positive or normative as it seeks to both analyse as well as formulate the foreign policy of a particular State. Apart from political science, I.R. draws upon diverse fields such as economics, history, law, philosophy, geography, sociology, anthropology, psychology and cultural studies. It involves a diverse range of issues, from globalisation and its impact on societies and State sovereignty to ecological sustainability, nationalism, economic development, nuclear proliferation, terrorism, organised crime, human security, and human rights.

It is interesting to note the changing dynamics of diplomacy in international affairs. Traditional diplomacy is the art or practice of conducting I.R., as in negotiating alliances, treaties, and agreements carried out by chosen diplomats of sovereign States. Public diplomacy is the new age diplomacy and a recent phenomenon, which deals with the influence of public attitudes

on the formation and execution of foreign policies. It encompasses dimensions of I.R. beyond traditional diplomacy; the cultivation of public opinion by governments, in other countries; the interaction of private groups and interests in one country with those of another; the reporting of foreign affairs and its impact on policy; communication between those whose job is communication, as between diplomats and foreign correspondents; and the processes of intercultural communications. Central to public diplomacy is the transnational flow of information and ideas.[1]

The interconnections of S&T with foreign policy and diplomacy are age old, but have never been more important than in the globalised, multi-polar world of today. Many of the defining challenges of the 21st century—from basic human security to the concerns of global climate change, from security of outer space to security in cyber space—all have scientific and technological dimensions. These are global issues and no one country will be able to solve these problems on its own. The tools, techniques and tactics of foreign policy of nations need to adapt to this changing world of increasing scientific and technical complexity.

Science and technology plays a key role in establishing the power-balance dynamics between sovereign nations. It offers alternative channels of engagement among countries that may have political differences, thus playing an important role by influencing the dynamics of power-balance between sovereign nations. Advances in S&T have often relied on international flow of people and ideas and this is happening now more than ever before. Even during the cold war, exchange between scientific organisations and universities were an important conduit for informal discussions on nuclear and other sensitive technology issues.

Different aspects of the role of science, technology and innovation in foreign policy, diplomacy and I.R. can be viewed in terms of three different dimensions of science diplomacy:

- Science in Diplomacy—using scientific advisory to achieve foreign policy objectives.
- Science for Diplomacy—using S&T cooperation to improve relations between countries.
- Diplomacy for Science—facilitating international scientific cooperation, and getting foreign S&T inputs for indigenous progress.

Probably one of the best examples of science in diplomacy—a mechanism for informing policymaking with scientific advice on a problem of global

dimension—is the Inter-governmental Panel on Climate Change (IPCC), established in 1988 by the World Meteorological Organisation (WMO) and the United Nations Environment Programme (UNEP). The mandate was to provide the world with a clear scientific view on the current state of climate change and its potential environmental and socio-economic consequences. In December 2007, the IPCC was awarded the Nobel Peace Prize (jointly with former US Vice President Al Gore) 'for their efforts to build and disseminate greater knowledge about man-made climate change, so as to lay the foundations for the measures that are needed to counteract such change'.[2]

Science for diplomacy comes into play on sensitive issues of national security, where collaboration between scientists can help to facilitate political negotiations. The soft power of science and the universality of scientific methods can be used to diffuse tensions even in 'hard power' scenarios, such as those relating to traditional military threats. For example, technologies to verify nuclear arms control agreements were a rare focus of joint working between the US and USSR during the cold war. Scientific enterprise is now premised on the need to collaborate and connect. Globally there are today invisible groups of researchers who collaborate, not because they are told to, but because they believe that they can offer each other complementary insight, knowledge and skills for the ultimate good for mankind.

Establishing and nurturing links between the scientific and foreign policy communities informs scientists and policy makers alike, the former about the realities of policymaking; and the latter about the role and limits of science in policy. Improving the scientific capacity of delegations from all concerned countries has become particularly important, especially for international negotiations on human health and climate policy. This is indeed quite a change.

The other dimension of science diplomacy, diplomacy for science, seeks to facilitate international cooperation, whether in pursuit of top-down strategic priorities for research or for bottom-up collaboration between individual scientists and researchers. Flagship international projects, such as the 'International Thermonuclear Experimental Reactor' (ITER) in France and the 'Large Hadron Collider' (LHC) projects are good examples where diplomacy has been successful in multinational teams for a major common scientific objective.[3]

Although these projects carry enormous costs and risks, they are increasingly vital in areas of S&T which require large upfront investments in

infrastructure, beyond the budget of any one country. However, such projects are the visible tip of the iceberg where bottom-up collaboration at various levels takes place between individual scientists and institutions. The stereotype of the scientist as a lone genius no longer holds true. Much of technology innovation is now happening with expertise pooled from many nations and major corporate entities are seeking 'co-innovation' potential across different nations.

As noted above, scientific values of rationality, transparency and universality are same the world over. Thus, they can help to build trust between nations. S&T cooperation therefore provides a non-ideological environment for the participation and free exchange of ideas between people, regardless of cultural, national or religious backgrounds. Hence, for foreign policy experts, S&T collaboration between nations offers potentially useful networks and channels of communication that can be used to support wider policy goals. The scientific community often works beyond national boundaries on problems of common interest, and is thus well placed to support emerging forms of diplomacy that may require non-traditional alliances of nations. If aligned with wider foreign policy goals, these channels of scientific exchange can contribute to coalition-building and conflict resolution. However, one must avoid the undue politicisation of science.

Historically, science diplomacy has proved very useful for confidence building among nations in conflict, when trust deficit becomes a major hurdle for progress towards peaceful resolution of conflict. Dialogue between the US National Academy of Sciences (NAS) and the Soviet Academy of Sciences during the last phase of the cold war was instrumental in facilitating the eventual dialogue between President Ronald Reagan and Soviet President Mikhail Gorbachev.[4] As such, much of the problems associated with the nuclear non-proliferation agenda could be discussed more constructively, through such science diplomacy.

Governance of international space beyond national jurisdiction, for peaceful use of outer space has been possible only through successful application of science diplomacy among space-faring nations. Scope for future science diplomacy is increasing steadily as we face increasing challenges of global dimensions that will demand global cooperation, even as individual nations may remain locked in strong competition. The world has also become much more interconnected and interdependent even during peacetime, and it is clear that that the strategies and tools of addressing major issues will be

influenced significantly by the techno-economic priorities of individual nations.

Interest in science diplomacy is growing at a time when I.R. is changing. The tight control on technology transfer by national governments is waning and multilateral institutions, multinational companies are playing a larger role than in the past. Technology diffusion is becoming unavoidable in the globalised world where economic competition is dictating the transnational interactions. The result is a more complicated and disaggregated diplomatic system, where besides the foreign policy experts representing their governments, we now have networks of technology experts, policy professionals, NGOs, corporate entities, and of course, the media interacting with each other, in any international forum.

A good example of this multilateral exchange for addressing a problem of global dimensions was the Copenhagen climate change conference in December 2009 (COP15). This was primarily designed to enable negotiations between national delegations from 192 countries, including 100 world leaders. But nearly 18,000 delegates from a vast array of NGOs, business, regulatory, scientific and media groups also attended the summit and contributed in numerous ways to its important outcomes that recognised the need for urgent quantitative commitment to mitigating climate change from major contributors to global warming over the past five decades. This is discussed in detail in a later chapter.

The security scenario around the world has undergone a profound change. Threat perceptions and national security interests now differ significantly for different regions and the threat of all-out war between major nations seems very remote. For over 40 years the Soviet-US confrontation dictated global security perceptions and hence, diplomatic priorities were intimately linked to balance of security. During this period, technological deterrence and diplomatic strategies dominated the delicate security balance quite successfully, as can be judged from the fact that, apart from a small number of war-alert situations such as the Cuban missile crisis of 1962, the two superpowers, even with their hair-trigger readiness for war, managed to avoid conflict through the well-calibrated Mutually Assured Destruction (MAD) doctrine.[5]

Looking back, this deserves to be recognised as a major success of bilateral diplomacy of the time that managed all kinds of relational issues between the two groups of nations that were essentially staunch adversaries. The technology for official diplomatic dialogue, Track-II exchanges, electronic espionage

networks, technology of surveillance and secure communication—all this made a real-time balancing act possible for the foreign policy experts from both sides.

It is interesting to note that since the end of World War II in 1945 till the turn of the century, over 200 smaller armed conflicts have been fought in the world but almost all of these took place in the developing Third World regions. Clearly, these countries which did not have either technology of high sophistication or any diplomatic experience, could not avoid regional wars. Most of these limited wars have been about border disputes or religious/ethnic conflicts that remained confined to their specific areas without escalating or endangering international peace. It may however be surmised that presence of two most important tools of avoiding war—preventive diplomacy and deterrent technology could have prevented many of these wars.

Science diplomacy is now shifting to the new multi-polar world order, with increasing number of government as well as corporate networks operating simultaneously, for sharing and collating information on common interest or common threat, for policy coordination, enforcement cooperation agreements, and formulating internationally accepted rules and norms on various contentious subjects. The efforts to define and strengthen the role of S&T within this shifting architecture of governance and diplomacy are still at an early stage. According to Bernice Lee of Chatham House, "Environmental threats are adding to the complexity of international relations in an already turbulent world. The anticipated bottlenecks and constraints—in food, water, energy, and other critical natural resources and infrastructure—are bringing new geophysical, political and economic challenges, and creating new and hard-to-manage instabilities."[6]

Given the advances in space technology, many areas of peaceful use of space are increasingly becoming double-edged. It is interesting to note that almost all space explorations and advances have national security concerns as the major motivation. Satellite technology capabilities have major dual-use potentials and modern society has already become very dependent on satellite-based systems for every international interaction. As the vulnerability of the satellite system has now become a strategic priority, technological capability for protection of such systems is critical for all space-faring nations. Hence, it is no wonder that space applicable weapons already exist, and there is potential danger of wrong use of this technology, that can forever destroy long-established norms to preserve the outer space for peace and benefit of all mankind. This represents yet another dimension of the science diplomacy

challenge—how best to prevent misuse of advanced technologies that can unwittingly topple the delicate balance of technology in space.

Cyber space is another emerging dimension of security and diplomacy where exploding technological advances of the present day have made it possible for an individual or a small group to threaten a full size State apparatus. The new digital world represents a paradigm shift from a very structured and government-controlled international environment. The emerging information age is indeed ideal for the expanding human expertise to get more transparent and orderly for common good; yet, the same technology and innovative adaptation by those with wrong intentions or destructive minds, can combine easily to cause debilitating disruption or devastation. Devious minds can plan to use every-day technology very imaginatively to create a huge adverse impact on the security and well-being of a large population, as was evident by the September 2011 terrorist attacks in New York and Washington. While diplomacy with terrorist groups is ethically unacceptable, technology can today provide means of coercive action to pre-empt such threats. All these represent a world of new challenges for diplomacy and I.R. where technology will play an increasingly decisive role.

Interplay of Science and Technology with Foreign Policy

Foreign policy dictates how a country will act with respect to other countries politically, socially, economically, and militarily. Foreign policy thus, essentially defines how a nation may relate to other nations in international affairs, which can impact its bilateral or multilateral relations with other nations or groups of nations. Diplomacy then becomes the means for the conduct of foreign policy, for establishing the points of contact with other nations in many dimensions of I.R. Historically, the focus of I.R. or diplomacy has been on protecting one's own security vis-à-vis other nations and resolving conflicts of interest for avoiding possible war. For instance, since the early days of humanity, on the plains of Africa, large tribes would presumably interact with each other through peace emissaries, to avoid engaging in all-out war.

Power is the fundamental factor in the calculus of I.R. It can be described in terms of mastery and control over key resources and capabilities to influence international affairs. In this case too, technology plays an important role in exercising control or influence. Foreign policy is handled by foreign ministers, government secretaries and ambassadors on diplomatic assignments in foreign countries, who have used every technological advantage available, to achieve

the diplomatic objective. However, the impact of technology is now increasing phenomenally in the modern world and leveraging technology for economic or political gains is becoming the norm. Technological knowledge is becoming an important component for retaining diplomatic effectiveness and for meeting challenges in global affairs. Foreign policy and diplomacy have always been important aspects of statecraft, but now the emerging 'knowledge society' demands that statecraft must include new sensitivities of the electronic medium that allow instant communication and information diffusion, thanks to the phenomenal reach and wide access of modern ICT.

Typically, diplomatic dialogue is often a process of resolving differences in perceptions and opinions through various stages of negotiations, to analyse and debate finer nuances and sensitivities related to the main point of difference. This is essentially a slow process that incorporates inputs from various stake-holders of both the parties and the attempt is always focused on defining priorities and margins for mutual adjustments. Perception of national power is indeed a major factor in diplomatic dialogue and more powerful nations with larger techno-military strength clearly have many advantages and are usually more successful in winning the argument.

However, advanced technology has brought in various new techniques for quick information dissemination and situational awareness on most sensitive issues and hence, the time slot for diplomatic dialogue is often much shorter than it used to be before. Espionage has always been a means to gain diplomatic advantage by gaining access to the other party's intentions and strategies, and has also been an accepted objective of diplomatic exchanges. Today, technology has made it possible to gain real time access to enemy communication and thus fine-tune one's own strategy in almost real time. The recent exposure of the US' tapping of phone and e-mail contents of thousands of individuals within the country and in other countries is a case in point.

Technical and economic cooperation are considered to be essential functions of an integrated and imaginative foreign policy. India's pro-Soviet inclination in the 1970s was deeply embedded in the technical assistance it received from the Soviets, while the West remained cold. Military-technical cooperation between India and Russia has been the centrepiece of their bilateral relationship and will continue to remain important in the years to come. Hence, technical cooperation is an indispensible component of foreign policy formulation and often plays a decisive role in defining foreign policy of a country. Presently, India's renewed interest in an alliance with Japan has its

roots in technological cooperation between these nations and also in a mutual political interest to counterbalance the rapid techno-economic rise of China.

Technological cooperation between countries is often a sign of an intimate and positive understanding between the actors. In 2005, the Indo-US civil nuclear energy agreement was witness to the transformation of these estranged democracies into strategic partners with enhanced cooperation. It sent out a clear message to the global political circles that India is now a trusted strategic partner of the US in Asia, with a subtle indication that India can emerge as a counter balance to China in South Asia. During this time, President George W. Bush had expressed deep interest in India becoming a stronger player in Asia. This has been discussed in detail in a separate chapter on game-changing technologies.

Transfer of technology is one of the major components of technical co-operation. In case of India, foreign direct investment (FDI) in Indian defence industries includes co-development, joint ventures and co-production of defence products and components. A good example of technological co-operation in the area of defence is the BrahMos, a supersonic cruise missile which is being co-produced by India and Russia. Technology transfer may also include FDI in government approved research and development (R&D) projects (recently expanded beyond the defence R&D). India already has an offset policy for the defence sector where foreign suppliers need to contract out at least 30 percent of the total value of the supplies locally. India is keen to ensure that its activities as a recipient serve its development as a producer.

Besides, the role technology plays in shaping hard power of a nation, i.e. defence equipment, infrastructure, manufacturing etc. and its consequent impact on foreign policy, it is also important to understand the role of technology in shaping soft power of nations and their foreign policy imperatives. The exclusive management of global public goods like the World Wide Web (www) is the most important instrument of American soft power in the 21st century. The internet relies on a global network of satellites, most of which are owned by the US Government. They have developed advanced terrorism intelligence systems that work in close tandem with high-tech satellites and equipment most proactively. In terms of education training and healthcare, the US has become the most preferred destination around the world. Foreign assistance through organisations such as United States Agency for International Development (USAID) and leading contributions to United Nations (UN) development activities have been a critical instrument of America's soft power. America is the most influential nation today and hence,

the most effective soft power. It has demonstrated that a nation with a large amount of soft power can often build coalitions and persuade other countries to comply with 'persuasion' rather than 'coercion', which is a harder version of soft power, almost bordering hard power.

In this context, it is also worthwhile to note that technical cooperation for development is an important instrument of soft power wielded by foreign policy experts. Sri Lanka is a telling tale of India's power projection in the region, especially in terms of 'soft-power' after the failure of its 'hard-power' approach in the past. Indo-Sri Lankan relations have dramatically changed in the last few years and embody the change in India's foreign policy perfectly. After March 2000, when the bilateral free trade agreement came into effect between the two countries, trade and its benefits have risen. National Thermal Power Corporation (NTPC) and Bharat Heavy Electricals Limited (BHEL) collaborated with the Ceylon Electricity Board to set up a coal power plant in Sri Lanka. Also, the Indian Railway Construction Company (IRCON) undertook six railway projects in Sri Lanka amounting to $800 million to reconstruct the railway lines damaged during the civil war in 2012. India is also involved in projects for renovation of Palaly Airport, Kankesanthurai Harbour, construction of a cultural centre in Jaffna, interconnection of electricity grids between the two countries, construction of a 150-bed hospital in Dickoya. Hence, technology cooperation in the areas of energy generation, electricity and infrastructure for development has enabled India to extend its soft power to Sri Lanka and similarly to neighbours like Bhutan and Nepal.

There have been ample examples of application of hard power with the help of advanced technology weapons to achieve foreign policy objectives. The successful application of high-technology weapons and techniques in US military operations in Iraq (2003) was a demonstration of how a world-class superpower could exercise its foreign policy over another far-away sovereign country, by first diplomatically convincing other major nations that there was credible threat of Weapons of Mass Destruction (WMD) and then using techno-military strength to devastate the target nation to change the political regime there. Without commenting on ethical or economic merits of the case, this was a clear case where even the UN was coaxed diplomatically to stand-by while the overwhelming techno-military power was used in a pre-emptive mode, without being provoked militarily.

Although the after-effects of the Iraq war became too costly for the US, the operation by itself was indeed a first-time success of the combination of technology and diplomacy that raised the US well above the rest of the world,

almost out of reach of even the second-best. With the help of latest technology, the US-led coalition was able to wage a high-precision war on a distant land to achieve its political objectives with ease. This signalled the new era of coercive diplomacy by a superior power to enforce submission of the weaker power. This is a trend that might find increasing relevance in regional power balance equations and also in enforcing cooperation for combined action against common issues such as global warming or space security etc. More powerful and high precision weapons along with modern network-centric strategies have dramatically reduced the time margins for diplomacy, thus making the risk of diplomatic breakdown all the more higher.

In this context, it is also relevant to understand the impact of technological revolution on foreign policy making. Just as information technology (IT) has permeated all aspects of daily life from business to entertainment to politics, so too its impact on the diplomatic arena. Increasingly States are recognising the role IT can play in enhancing diplomatic functions. The use of technologies such as e-mails, virtual and online conferencing at international negotiations, now make it possible for delegations to communicate in real-time with the home office for information on official positions, or for advice on formulating responses to unanticipated issues, and reactive diplomacy. The use of IT tools also enables resource-deficient States, which would otherwise be unable to attend many of these meetings to maintain a 'virtual' presence and to participate via electronic media. This feature could be important for the smaller developing States who often find it onerous to participate in international meetings and negotiations for the reasons previously outlined.

Another dimension worth consideration is the creation of *a Virtual Technical and Planning Facility* in which technical experts, trade professionals and experienced negotiators from the larger States can assemble under the direction of the respective ministries, for example, foreign affairs, to provide advice, critique strategies and simulate negotiation scenarios for the benefit of the less developed State. Simulation technology for scenario analysis is a major help in planning diplomatic strategies of major powers of the world today.

The nature and scope of diplomacy continues to be redefined as the international system evolves. As the information era unfolds, new actors are utilising IT and communication technologies to engage States in a new type of diplomacy, one driven by technology in which informational assets and real-time delivery are key components for desired outcomes. Developed nations have been quick to recognise that in the emerging diplomatic environment

new electronic mechanisms must complement existing approaches if they are to effectively reach 'net' constituents. Already the use of IT tools has become the norm at international negotiations, facilitating speedy communication and more comprehensive information gathering and analysis. The trend towards bloc negotiations further accentuates the use of IT in facilitating interchanges amongst member states.

Developing States predominantly situated in the South, are seeking to re-negotiate and redefine more tangible benefits for themselves in an international system whose institutions and theoretical underpinnings seem designed to promote the interests of the developed North. Effective diplomacy will therefore become the key to articulate and secure maximum benefits for the region as a whole. How successful the region is in obtaining desired outcomes will depend in large measure on whether it can utilise knowledge to target realistic outcomes, using innovative diplomatic strategies. Preparedness for negotiations, the region's ability to internationalise its causes and influence public opinion become key elements of the new diplomatic game. The use of IT tools and knowledge systems should be viewed as major assets to the region's diplomatic success in the future.

Advances in science and technology have become key drivers in I.R., and knowledge of trends in key fields is an essential prerequisite to effective international negotiations. Knowledge of trends in science and technology is also a key element for the successful national implementation of international agreements. There are two key features of the growth of scientific and technological knowledge that are central to the international negotiations. Firstly, scientific knowledge is becoming increasingly specialised and therefore demands greater input by the experts into international negotiations. Secondly, the application of science and technology to development requires the ability to integrate divergent disciplines that are needed to solve specific problems. International diplomacy now demands that government negotiators deal with both specialisation and integration.

Technology Controls and Foreign Policy: Indian Perspective

Historically, one of the classic cases of using S&T leverage for achieving foreign policy objectives has been the use of technology embargo against the adversary. It is less punishing than economic sanctions by a superior country against a less powerful country but the message or intent is very much the same—'if you are not an ally or a trusted friend, then you cannot benefit from my riches or technology knowledge'. It is in this context that one needs to

appreciate the role of technology controls in I.R. The origin of arms control can be attributed to the basic national security imperative to reduce both the incidence of armed conflict and the level of potential for damage in a conflict situation. Technology controls for preventing proliferation are often classified as for 'common good' of mankind, but a closer look shows that there can be significant differences in defining the 'common good' and hence it is very much a foreign policy perspective of individual nations.

The four broad objectives of arms control are: (*a*) to manage the techno-economic balance; (*b)* to reduce the possibility of war; (*c*) to reduce the consequences of war, if it happens; and (*d*) to optimise resources for defence so that economic development does not suffer unduly. Although technological advances have been instrumental to all human development, much in the same way as industrial revolution or mechanised warfare, they too have created modern weapons with greater potential to cause damage. To capture the process in its conceptual stage, it is possible to reflect on the 1899 and 1907 Hague Conventions, which banned the use of 'dumdum' bullets and the use of poison or poisonous weapons, and the 1925 Geneva Protocol for the Prohibition of 'Asphyxiating, Poisonous or Other Gases' even in war. Similarly, biological or chemical methods of warfare are also banned by general consensus by the world community.[7] These early efforts to limit the development and acquisition of dangerous weapons came to be identified as arms control.

The concepts of 'technology control' became more relevant during the cold war through the sharper focus on non-proliferation of NW. It was a clear signal that as technology gets more devastating it would be very critical to control such technologies. The initial objective of the Nuclear Non-Proliferation Treaty (NPT)[8] was to prevent proliferation, both horizontal (spreading to other nations) as well as vertical (enhancing the quantity or quality of WMD within the NW holding nations) so that devastating WMD could remain under the tight control of the five countries that acquired it before the international treaty was finalised and brought to force. The NPT objective included arresting growing dependence on NW, for eventual elimination of NW by all. However, dependence on NW grew astronomically during the cold war, with both super-powers building NW arsenals by thousands. Realising that the growing importance of NW for strategic superiority would make it very attractive for an increasing number of aspirants for the same advantage, the Nuclear Suppliers Group (NSG) [9] was formed in 1975, for establishing tighter control on supply of NW related technologies

and items. During this time, supporting initiatives, such as the Zangger Committee, were also evolved to create a listing of control items and technologies that can serve as a guide for non-proliferation efforts.

Ballistic missile technology emerged as a vital capability for long range delivery of WMD and thus the need to control the WMD threat intrinsically included control of missile technology. However, the 'dual-use' nature of technologies for military missiles and civilian space launch rockets brought-in new challenges for the managers of international affairs, to define what level of dual-use technology was considered safe or internationally harmless, with which nations. The secret gathering of seven industrial nations (the US, the United Kingdom, France, West Germany, Canada, Italy and Japan) formulated the Missile Technology Control Regime (MTCR) in 1983.[10]

The concept found very useful application to the foreign policy objective of denying modern technology benefits to adversarial nations towards maintaining techno-military superiority over the enemy. The US-led Western alliance took the major lead in establishing rules and regulations for technology control to serve two very distinctly separate objectives—one to prevent nuclear proliferation, and the other, to serve the foreign policy objective of denying the Soviet-led alliance the benefit of modern technology being developed by the US-led group of nations. All necessary organisational structures, frameworks and specially trained manpower were created to ensure strict compliance by coalition members and for stringent monitoring of country-specific verification and monitoring of dual-use technology interactions and trade. MTCR represented the power of collective diplomacy where an informal agreement among a set of powerful nations became fairly effective, without formally making it an official international treaty.

All through the cold war decades, both the superpowers invested heavily in R&D for advanced military technology. In the NW arena, technological advances for NW sophistication, as well as enhancing the range and accuracy of their delivery vehicles, became the central focus of various technology denial regimes. Although MTCR was not an international treaty, it found support from many other nations under missile threat and became a sort of benchmark for technology controls by the late 1980s. While the focus was on long-range missiles with potential nuclear warheads, the 1991 war against Iraq produced a new surprise by demonstrating that relatively old technology of short range 'Scud' missiles and even rockets/mortars can pose a serious threat to civilian population and change the security perceptions in neighbouring

nations. This was a new challenge for diplomacy and of course, also for the technologists to innovate new solutions for such short range, low level threats.

The MTCR guidelines were revised in 1993 to increase its effectiveness and more nations were encouraged to join the regime—taking the membership to 26 by 1993, and six others, including Russia and China promised adherence to MTCR without formally signing it. India continued to be among the target countries, although at a much less strict level, since the US-India civil-nuclear agreement of 2008 and subsequently the NSG accepting India as a responsible owner of technology. With change in international perceptions about India, it has now expressed its willingness to join the MTCR and other technology control groups as a partner, rather than a target. This is a major transformation of India, changing its status from target group to membership group, with prudent technology practice and very effective diplomacy, backed by foreign policy reforms to match international standards. The initial export-control regime of significance during the cold war years was the Coordinating Committee for Multilateral Export Controls (COCOM)[11] which was a technology embargo regime to prevent the transfer of dual-use technology and equipment to communist bloc States in the belief that such equipment and technology, if diverted to military use, could have contributed significantly to the military potential of the adversary. In June 1992, seventeen countries participating in COCOM decided to establish a cooperation forum to define a successor regime for future technology controls. The cooperation forum, which did not immediately replace, but at first existed alongside COCOM, had four objectives.

These were: (*a*) to significantly ease access by East European countries to advanced goods and technology; (*b*) to establish procedures to ensure against diversion of these sensitive items to military or other unauthorised users; (*c*) to assist the East European States to develop their own export control systems; and (*d*) to provide a mechanism for further cooperation on export control matters. COCOM continued to exist as a 'Cooperation Forum' for the next three years, while an alternative arrangement was under discussion. During this period, the number of items on the COCOM control list was progressively reduced (and these items were no longer subject to embargo) and by 1996, several countries that had been the targets of the embargo were friends and important trading partners. There was then an active discussion to enlarge the North Atlantic Treaty Organization (NATO) to include some of them as members. In 1996 the Wassenaar Arrangement emerged as an informal technology-control arrangement of member-states.[12] The objectives of

multilateral export control regimes typically include commitments: (*a*) to regulate sensitive technology transfers with potential military applications; (*b*) to introduce a licensing mechanism to institutionalise export controls; (*c*) to create a database for mutual information sharing for better coordination of controls; and (*d*) to identify countries of concern and prevent the proliferation of dual-use technologies to them. Today, in the changed multi-polar world, technology control effort remains the responsibility of individual nations under the overarching consultative process of the control group. This indeed represents the new international reality that ultimately, success of technology control and prevention of technology misuse will depend on the record of a nation's ability for responsible ownership of sensitive technology. Discussion of such 'Responsible Ownership of Technology' can be found in this author's earlier monograph *Technology and Security in the 21st Century* published by SIPRI in 2004.[13]

New Technologies and New Concerns

The last decades of the 20th century witnessed phenomenal advances in military technologies. The post-1945 superpower competition drove a technology race that produced amazing results in a short time span. While the doctrine of MAD now seems irrelevant, new threats have surfaced *inter alia* because of the worldwide spread of religious fundamentalism and terrorism. The unavoidable diffusion of advanced technology has led to new and grave concerns regarding WMD technologies proliferating into irresponsible or extremist hands. Since these non-state organisations operate ubiquitously without national borders, it is a new type of asymmetric threat that cannot be contained by military power alone. This is where S&T can provide valuable intelligence and information for diplomacy to act decisively.

The rapid progress in IT during the past decade alone has opened up several new possibilities for using technology for strategic or operational advantages. Increasing computing speeds, smaller hardware and innovative software approaches are creating even more options. IT has already revolutionised the battlefield, with the trend of network-centric command and control philosophies that dramatically reduce the 'sensor-to-shooter' time of response. Instant information access and real-time inputs about battlefield conditions at the level of foot-soldier has transformed the close-combat scenario to a digitised format that can be readily useful for deployment of efficient robots that can replace humans in extreme hazardous situations.

Another major new technological trend in matters of defence and security

is the increasing use of outer space capabilities for enhanced performance and stand-off ranges. Ever since the announcement of the Strategic Defense Initiative (SDI)[14] by the then US President Ronald Reagan in 1983, the impact of technology on defence strategies and operational doctrines has changed dramatically. With vastly superior technologies of long range high-precision missiles and space based Ballistic Missile Defence (BMD) the US was able to have enormous deterrence capacity to which the very powerful Soviets had to give-in. Advances in military space capabilities have sharpened situational awareness to a level that major powers of today are able to anticipate most dangers to their security and take preventive steps to nullify the threat. The US' use of Unmanned Aerial Vehicle (UAV) technology for targeting small specific terrorist groups, sitting in secure command centres on the US mainland—represents a quantum leap in technological capabilities in the future war scenario. However, it must be borne in mind that some amount of technology diffusion is inevitable and future concerns must include the possibility of such advanced technologies being available to rebel groups or State-sponsored fundamentalists.

Many of the science fiction projections of the yester-years are close to realisation and the impact of these technologies on future security strategies is likely to be very profound and long-lasting. Space is already being used extensively for military purposes and robotics, and artificial intelligence advances are enhancing the capabilities of robotic systems. Aerospace vehicles that can rise directly to space orbits are near maturity. The robotic space plane XB-37 has already made successful long duration flights. The introduction of directed energy weapons and possible increase in the military exploitation of satellite systems for combat purposes will revolutionise the future trial of strength between powerful nations.

The latest trends in technology development for military purposes also indicate a move towards miniaturisation, improved efficiency and greater flexibility. As weapons become smaller and more efficient, deployment strategies and operational scenarios become more flexible, making a large variety of options available to the user. The shrinking size and weight of strategic warheads are a classic example of how technology has made the attacker's job easier and the defender's job more difficult—creating more demand for newer technology options to meet the new level of threat. It is also interesting that, with the increasing accuracy of weapon delivery technology and the increasing lethality of new warheads, there is growing interest in the development of non-nuclear strategic weapons. Technology

controls of the cold war era are not going to be effective in all such dual-use technology areas where technology diffusion is very rapid and widespread, essentially because these technologies are also very important for economic competitiveness.

While much has been done to establish architecture for international arms control with the intention of ensuring international security and peace, the question remains as to how far they have been successful in the final analysis. At the height of the cold war, most analysis of security cooperation was focused on bilateral US-USSR arms control. However, today, most of the focus has shifted to multilateral agreements and in the multipolar world of today, new challenges are emerging every day to threaten the existing arms control regimes. Hence, a new approach to international technology management and disarmament may be what is needed for the future.

Often, discussions and lack of consensus among practitioners provide the incriminating evidence of the partial success with the threats and dangers of proliferation. Although treaties such as the NPT or initiatives like the MTCR have made important contributions to slow down proliferation, their success remains limited. Largely, the international global arms control architecture has become rather obsolete and a somewhat static regime, solidifying prevailing inequities or a status quo that will not stand the test of time. Some States are bound to reassess their commitments or hesitate in making new commitments in nuclear or other sensitive areas. As long as there is discrimination between nations and regions in terms of access to earth resources and in the context of the Human Development Index (HDI), a simmering tension will prevail among the less privileged who will aspire for technological means to better security and prosperity. Ultimately, regional and international peace and security will run the risk of being jeopardised by misuse of technology, by irresponsible or rogue elements that benefit from failure of technology controls.

The lack of confidence in the present arms control regime and in its ability to contain possibility of war is evident in the increasing demand for WMD. The West Asian region is a striking example of the failure of international and regional non-proliferation efforts. The continuance of nuclear-missile proliferation trends in West Asia with the possible emergence of any new Nuclear Weapon State (NWS) will have a fundamental effect on the security paradigm in the region. In fact, every single Arab country joined the NPT as a Non-Nuclear Weapon State (NNWS), and each, with a potentially significant nuclear programme, has a full-scope safeguard agreement in place with the International Atomic Energy Agency (IAEA).[15] Yet, very significant questions

remain regarding the present state of play of nuclear proliferation in the region. The number of international proliferation outbreaks over the last decade is an alarming testimony to the diminishing relevance of global arms control regimes and there has been a failure to curb the desire for NW.

India of course, openly declared itself a NWS in 1998 when NPT totally failed in India's neighbourhood, with China, itself a NPT member, but blatantly supplying NW and missile technology to Pakistan. During 1970 to 1990s, India observed exemplary restraint and technology maturity while neighbouring Pakistan became a hub for nuclear proliferation with the famous AQ Khan network.[16] Since the US was heavily dependent on Pakistan in the war against terror, it chose to overlook Pakistan's clandestine proliferation and eventually even made Pakistan a non-NATO ally. It is in this backdrop that India focused on indigenous development of high-end defence technology of nuclear-missile weapon systems as credible deterrence with minimum investments.

The record of non-proliferation and nuclear disarmament till date is not very impressive. The international community has failed to deal with these issues in a manner commensurate with their importance, or the dangerous ramifications of failures in these realms. As global citizens and stakeholders of a collective international security, it is important for India to analyse reasons for this failure. Firstly, there is lack of strict compliance to international treaties by major powers in international politics. The problems facing multilateral export controls do not lie primarily in the flaws in the structures of the existing agreements (though improvement in implementation is always desired). Current difficulties emerge from the practice of using technology for short-sighted foreign policy gains, especially by major powers.

Compliance with the MTCR by all its members remains questionable. The Wassenaar Arrangement based on the principle of consensus has proved more difficult to enforce. China, an emerging military power, is a participant in most arms control agreements but its record of adhering to promises in the realm of arms control is not at all impressive. Earlier, the withdrawal of the US from the bilateral 1972 Anti-Ballistic Missile (ABM) treaty[17] with Russia was another example of how major powers routinely flout international commitments when national priorities over-ride common good. While this paved the way for the US' pursuit of its BMD programme without any formal restrictions, it also led to proliferation of missile defence technology by many powerful countries, which in turn can have a de-stabilising effect on the balance of deterrence.

Secondly, a major concern is the shift of US policy to 'Unilateralism'. This has the potential to undermine the fabric of international agreements that form the basis of any compliable policy. The Comprehensive Nuclear-Test-Ban Treaty (CTBT), which is one of the best mechanisms for disarmament in terms of details of provisions, verification measures, and regime strengthening, was rejected by the US, even though it faced no great power as a rival in the near term. The international attempt towards disarmament was again turned into an instrument for discriminating arms control. This is significant because if even one of the strongest disarmament measures is not deemed worthy of acceptance, then there is a problem with the very idea of arms control rather than its specific provisions.

The continued pursuit of BMD by the US is bound to encourage players like Russia and China to adopt a more offensive posture in order to neutralise the advantages of BMD. The Chinese reaction to the American BMD can be seen in their focus on rapid development of space technologies and counter-space capabilities. China's continued plans for military modernisation are now set to match US capabilities. How this affects the US-China relationship and impacts China's immediate neighbourhood, will also determine the future of international stability in general and India's security in particular.

The very nature of these arms control agreements fostering inequity and discrimination has been criticised and rejected by the countries in the developing world. A partial disarmament cannot ensure international security for all nations. It is worthwhile to note that some of the first five NWS have been instrumental in spreading nuclear technology and components to other aspirant countries. Hence, indirectly, they are responsible for contributing to the proliferation of nuclear-missile technology and accentuating the threat from WMD around the world. The failure of the global arms control architecture can be attributed to the loose structures of these multilateral agreements where powerful nations could favour friends and punish adversaries while holding a high moral ground. The future demands an objective approach for effective dual-use technology management and export control systems.

An effective export control system must have robust 'Legal Framework' that consists of legislation for controlling strategic exports, including specific civil and criminal penalties for violation, clear licensing procedures, establishment of regulatory practices and creation of control lists of goods, services and technologies consistent with multilateral norms. A comprehensive verification system under a global body such as the UN is necessary to monitor compliance in terms of detecting intentions to break laws and treaty

commitments. Effective enforcement mechanisms are required that can encompass adequate awareness, training and empowerment of customs personnel and border guards to recognise, inspect and interdict strategic control list items. India is simultaneously engaged in all these processes, as is expected of a responsible international technology player.

More than ever in the past, the effectiveness of trade controls to sincerely check proliferation has become very critical now. Minimising dangers of WMD terrorism depends on their acceptance and enforcement by all countries, and particularly by those with the capacity to deal in dual-use items and technologies. India's participation in this endeavour, despite not being a member of the non-proliferation regime, is critical. India, until now having chosen to remain outside such regimes, has a special significance as a new NWS and major user, producer and trader of dual-use items and technologies. In this context, it would be important to understand India's past and present approaches to export controls, identify measures towards their better institutionalisation and to deliberate on measures for building confidence for India's international trade and national security.

From being a target of technology denial regimes in the past, India has emerged as a responsible owner of sensitive technology with a clean record of preventing proliferation. For Indian administrators and diplomats, it is crucial to understand that besides raising its international credibility, the effective implementation of trade controls also directly serves the cause of India's national security. Through the 1990s, the changing character of Indian exports from a largely agricultural or raw material content to a greater proportion of IT services, manufactured goods, technical know-how and electronic components and assemblies—indicate a very healthy trend. India is now a user and producer of a range of dual-use materials, equipment and technologies; thus a partner in global affairs.

There is also an increasing participation of the private sector in high-tech areas of defence industrial sectors. Unlike government entities that have been major players in the past, and on which it was possible to exercise strict centralised control, the new corporate entities need to be regulated with an updating of legal and procedural mechanisms. To make India a major player in high-end technology and systems, it is important to strengthen strategic trade controls in order to raise confidence in the exporting nations that the received technology or materials would not be in danger of falling into the wrong hands. Consequently, national trade controls provide the international community with the necessary confidence and guarantees against unauthorised

re-export and diversion. In all the above, it is important that foreign policy and technology management are fine tuned to complement each other.

In terms of regional threats, revelations about the reach of the sophisticated network of illicit nuclear commerce in Pakistan have raised new concerns about diffusion of nuclear technology into wrong hands and possible nuclear use or threat of use by non-state extremist actors, with or without State support. It has raised new questions on effectiveness of nuclear deterrence in the region. Given presence of such sophisticated clandestine networks, one cannot rule out the possibility of dangerous technologies reaching terrorist groups. The perception that Pakistan is reducing its nuclear threshold by developing tactical NW is very alarming for India and an even greater worry is the suspected involvement of Chinese scientists helping Pakistan in its endeavour to challenge India with its new nuclear toys. For the present, it appears that the Pakistan Government has been able to build a more credible deterrence against India, while India with its no first strike policy and an apparent lack of will to take on Pakistan diplomatically, has lost the race for enforcing a credible nuclear deterrent in the region of immediate interest to India.

In conclusion, one may state, it is time that the international community realises that selective or limited solutions to proliferation or disarmament concerns will not meet with desired long-term success. India along with older nuclear powers should rise to the challenge and offer ideas on a new framework for international security that is suitable for the 21st century. There is a need to rekindle the multilateral agreements on international security with more objective and stringent norms for compliance. India should emerge as a major responsible player in the game.

NOTES

1. "New frontiers in science diplomacy : The changing role of science in foreign policy", *The Royal Society*, January 12, 2010, at http://royalsociety.org/policy/publications/2010/new-frontiers-science-diplomacy/ (Accessed June 7, 2014).
2. The Nobel Peace Prize 2007 was awarded jointly to the Intergovernmental Panel on Climate Change (IPCC) and Albert Arnold Gore. See www.nobelprize.org/nobel_prizes/peace/laureates/2007 (Accessed June 7, 2014).
3. ITER is an international project to design and build an experimental fusion reactor based on the "tokomak" concept. "ITER—the way to new energy". See www.iter.org/ (Accessed June 7, 2014).
4. "US-Soviet Scientific Cooperation in the Age of Confrontation", at www.nap.edu/openbook.php?record_id=10888&page=1 (Accessed June 7, 2014).
5. Michael Shermer, "Will Mutual Assured Destruction Continue to Deter Nuclear War?" *Scientific American*, June 1, 2014 at www.scientificamerican.com (Accessed June 7, 2014).
6. Bernice Lee, et. al., "Accelerated environmental degradation and rising political tensions",

Resources Futures, *Chatham House,* December 1, 2012 at www.chathamhouse.org/publications/papers/view/187947 (Accessed June 7, 2014).

7. The international community banned the use of chemical and biological weapons. International Committee of the Red Cross, January 12, 2014, at http://www.icrc.org/eng/war-and-law/weapons/chemical-biological-weapons/ (Accessed June 7, 2014).
8. The NPT is a landmark international treaty with an objective to prevent the spread of nuclear weapons and weapons technology. "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)". See www.un.org/disarmament/WMD/Nuclear/NPT.shtml (Accessed June 7, 2014).
9. The Nuclear Suppliers Group was established in 1975, and comprises 46 nuclear supplier States. See http://www.armscontrol.org/factsheets/NSG (Accessed June 8, 2014).
10. "MTCR Guidelines and Annex" at fas.org/nuke/control/mtcr/text/mtcr_handbook_guide-annex.pdf (Accessed June 8, 2014).
11. "Multilateral Export Control Policy: The Coordinating Committee (*CoCom*)", at http://www.princeton.edu/ota/disk3/1979/7918/791810.PDF. (Accessed June 8, 2014).
12. The Wassenaar Arrangement Control Lists, Summary of Changes Adopted, at www.wassenaar.org/controllists/ (Accessed June 8, 2014).
13. Amitav Mallik, *Technology and Security in the 21st Century: A Demand-Side Perspective*, SIPRI Research Report No. 20, Chapter 5, Oxford University Press, New York, 2004, pp. 131-135.
14. The SDI, was a programme first initiated on March 23, 1983. "The Strategic Defense Initiative (SDI): Star Wars". See www.coldwar.org/articles/80s/SDI-StarWars.asp (Accessed June 8, 2014).
15. The Agency's activities are carried out to help States strengthen their nuclear security. "Nuclear Safety and Security", IAEA at www-ns.iaea.org/security (Accessed June 8, 2014).
16. "Nuclear Black Markets: Pakistan, A.Q. Khan and the Rise of Proliferation Networks—A Net Assessment", May 2, 2007, at www.iiss.org/nuclear-black-markets—pakistan—a-q—khan-and-the-rise (Accessed June 8, 2014).
17. Department of State, "Anti-Ballistic Missile (ABM) Treaty", Arms Control Association, at http://www.armscontrol.org/documents/abmtreaty (Accessed June 8, 2014).

2

Technology and Security: Challenges for Diplomacy

Introduction: Technology, Security and Diplomacy Interplay

Growth of science and technology (S&T) in India has been slow but steady. Rising out of 200 years of foreign occupation, independent India had to focus on societal development, food, hygiene and education etc. on high priority. Hence, foreign policy formulation started with a cautious and non-confrontational, non-aligned approach. The initial decades saw extensive application of S&T for nation-building and human development. Hence, early investments made in agriculture, energy and space technologies yielded handsome returns for nation-building; the 'Green Revolution' of the mid-1960s is a shining example. Focus on defence technologies came only after the bitter experience of war with China in 1962 and another war with Pakistan in 1965.

However, India was quick to enhance its defence preparedness with help from the erstwhile Soviet Union and demonstrated its regional power capability in the 1971 war with Pakistan that created Bangladesh. It was indeed a stellar success of a well-coordinated military operation supported ably with strategy, diplomacy and technology. For young India, this was a classic case of clear recognition of its national security threat that was addressed with sound strategic planning, a prudent foreign policy alignment with the Union of Soviet Socialist Republics (USSR) and a well-coordinated military operation. What

was also on display was the political will of the Indian leadership that did not wilt even in the face of US warships threatening counter-action.

Soon, India got down seriously to developing indigenous S&T capabilities to strengthen military capacity, and within two decades, India was already chasing self-reliance in critical technologies that were denied to it by the Western group of advanced countries. The early research and development (R&D) in atomic energy, space technology and defence systems was instrumental in creating the S&T base in the country that enabled the nation to become a major S&T force in the region. Within three decades after 1971, India produced an indigenous missile force, launched numerous indigenous satellites and also conducted a series of nuclear weapon (NW) tests to claim grudging international acceptance as a NW country.

With changing international geopolitics, India even realigned its foreign policy suitably to be recognised as a constructive international player, as was evident in the successful Indo-US civil nuclear cooperation agreement by 2008. From being the prime target of the NPT regime in the mid-1970s, to opposing the NPT extension in 1995 and the Comprehensive Test Ban Treaty (CTBT) imbroglio soon thereafter, India has conducted itself remarkably to stand as a de-facto Nuclear Weapon State (NWS) and an active international player on nuclear energy issues. This shows that when pushed to perform, India can rise to the occasion on matters of supreme national security interests. The new Indian Government, post the 2014 elections, is showing great promise for enhancing India's international clout in many direct as well as subtle ways.

It was a combination of technology, strategy and diplomacy that made India what it is today. India could have progressed much faster but for the constant pressure on its resources, and the attention required for fighting low-intensity conflict, against Pakistan sponsored terrorism and strategic encirclement by China that does not want to see India gain any techno-economic strength. China with its autocratic political system was able to grow faster in a synchronised manner, while India remained mired in problems of coalition politics, of democracy and consequent difficulties in decision-making. Notwithstanding the disadvantages, India still is a classic example, where indigenous and collaborative S&T efforts were oriented to strengthen defence and deterrence capabilities against adversaries and for building diplomatic bridges with friendly nations, for rapidly overcoming weaknesses in defence technology.

For many decades, technology development in India has been need-based and not really driven by any 'Grand National Plan'. As a result only 'need'

has been in focus, while technology was perceived just as an instrument for meeting those needs. Even so, there were no long-term plans for synchronising technology development or technology acquisition with the objectives of foreign policy or diplomatic agenda. As a compulsive buyer, India has been getting yesterday's technologies at tomorrow's prices and hence, lagging behind most of the developed countries, with consequent diplomatic disadvantages in I.R. A review of science and technology in India by the author can be useful for getting a comprehensive idea of the Indian S&T scenario.[1]

While there have been many pockets of excellence in scientific research and technology innovation, the nation as a whole still fares rather poorly in S&T in comparison to most other comparable nations. This is despite the fact that potential for much higher performance in S&T is very high, if progressive reforms were to be brought-in from time to time in an integrated manner, with long-term security priorities. India also performed very poorly in implementing the S&T policy decisions with the urgency and professionalism that could have made the country globally more competitive.

Early international cooperation for advancing S&T in India saw the establishment of Indian Institutes of Technology (IITs) in collaboration with the United States (US), United Kingdom, Soviet Union, Germany and United Nations Educational, Scientific and Cultural Organisation (UNESCO) for basic applied science and technology. Cooperation for the Canada-India atomic energy reactor for harnessing the atom for peaceful applications was yet another early diplomatic success for technology acquisition. However, the Peaceful Nuclear Explosion (PNE) of 1974[2] by India invited serious international disapproval and strict technology control regimes were used against it to deny almost all dual-use technology items and know-how. While some sensitive technology denials could be justified on account of legitimate nuclear proliferation concerns, India's close relationship with the USSR also made India a target of foreign policy-oriented denials for Soviet-bloc countries. Meanwhile, Indian Science Attaches posted at important Indian Embassies in a few leading nations, pushed for progress in S&T cooperation in areas of basic research and education that had little impact on defence and security technology cooperation.

It is interesting to note that restrictive technology denials became major motivating factors for India to strive for indigenous competence in critical technology areas. Although the overall pace of technology growth in India did slow down particularly for defence, space and atomic energy projects which faced denial from US and the Western alliance for every technical demand. It

was in this context that a major diplomatic initiative was taken by India to establish an office of Adviser, Defence Technology, at the Embassy of India in 1988. This was one of the first cases for India to combine the expertise of a defence technologist with the diplomatic experience available at the Embassy, to improve India's access to defence-critical technology. The groundwork done and the lessons learned proved very fruitful in reversing many high-tech denials to India and building the foundation for future US-India high technology cooperation.[3]

The unique advantage of combining S&T and diplomacy in bilateral efforts is that it enables building enduring techno-political bridges for serving the cause of furthering mutual national objectives. Notwithstanding the US-India spat during the 1995 CTBT negotiations and the furore over India's nuclear test in 1998, the Indo-US strategic partnership that could be rejuvenated by 2005, was the result of opening of windows for Indo-US cooperation through techno-diplomacy initiated in defence sensitive technologies.

The US-India civilian nuclear cooperation negotiated between 2005 and 2008 has been a major learning experience for foreign policy experts in both countries. In a strange way, India's political decision to go overtly nuclear in 1998, despite initial international outcry, opened-up new international avenues for diplomatic dialogue and eventually India did gain grudging recognition as a NW power. This enabled diplomatic initiative to renew high-tech cooperation with US and other powerful countries. India's policy clarity on strategic technology issues and its record of responsible behaviour with sensitive dual-use technology paid rich dividends in international high-tech cooperation. India has exercised unilateral control on sensitive dual-use technologies as a clear signal to the world that India is fully committed to non-proliferation of potential dangerous technologies. This has been a major diplomatic success for India in positioning itself on a strong footing for techno-military cooperation with other countries in the 21st century.

Impact of Technology on Politics and Global Affairs

Increased globalisation and rapid advances in technology have weakened national borders and enhanced technology diffusion. The information technology (IT) revolution and the spread of individual skill-oriented knowledge, make export controls almost impractical in some areas. Applying export controls to a large band of technologies and to all countries requires significant infrastructure to help make licensing assessments if implementation

is to be effective. The associated costs, combined with the opportunity costs from lost export earnings, could make export controls too expensive to justify for many nations.

As discussed earlier, technology diffusion and increased globalisation have made international transactions far more interdependent and market-driven than ever before and the trend is bound to accelerate as economic competition becomes sharper. Even clear-cut arms export controls have faced problems because of the pressures of the arms export industry. When it comes to controlling dual-use technologies, definitions of what can be exported safely, and to whom, becomes even more complex.* Export controls have remained subjective based on foreign policy perceptions of the supplier nation and often change with change of perceptions.

The technology denial regimes of the past five decades have spurred indigenous technology growth in many progressive countries. One of the major problems for export control regimes is the realisation that a number of countries outside the core regime, such as China, India and Israel, have become potential technology suppliers themselves. In addition to being important techno-economic players of the future, these countries are also potential markets for sales of high technology.

One of the major impacts of the IT revolution is the risk of cyber warfare. The new level of dependence on IT in every walk of life, including defence and security matters, has brought about a new vulnerability and a consequent new threat perception from the risk of cyber warfare at different levels. Unlike conventional military hardware that causes destruction and death, cyber warfare techniques use intangible software tools that can cripple military capabilities and international commercial trade. In a sense, they are full-spectrum techno-economic tools for use in both defensive and offensive strategies. The nature of this technology is making individual brainpower often more relevant than techno-industrial infrastructure. This is threatening to compromise the huge technological advantage that the Western industrialised nations have established with years of effort.

There are now new types of threat to an information-based society, where

* For example, Germany and Sweden are believed to have sold industrial electron beam machines to the Semiconductor Manufacturing International Corporation (SMIC), a Chinese manufacturer of computer chips. The US, however, is known to have banned such exports to China. It is an open question whether this is a case of undercutting the US or of disagreement over how to interpret agreed export control guidelines.

information security becomes as important as defence against a Weapons of Mass Destruction (WMD) attack. Technology has thus changed the nature of warfare from visible large-scale military action and violence to subtle, invisible yet decisive capabilities for crippling the enemy's information environment in a war-like situation, thus denying it the command, control, communications and intelligence (C^3I) advantages.

The ubiquitous nature of IT has also removed the clear distinction between covert and overt actions, because there is no clear, common, international agreement or even an understanding of acceptable and legitimate limits of using IT to protect national security interests. Paradoxically, it is the advances in sensor technologies and enhanced IT capabilities that are also responsible for enabling the technological edge necessary to counter WMD threats. IT can aid comprehensive monitoring and verification techniques for compliance verification as well as for early detection of proliferation activities, thereby complementing National Technical Means (NTM) for verification and monitoring. This will be valuable for the verifiable reduction or elimination of WMD arsenals and thus enhance confidence among the countries participating in co-operative disarmament. It is hoped that this will lead the world towards meaningful universal disarmament. Such ubiquitous technology as info-tech cannot be controlled even if it is subject to misuse by rough elements.

Biotechnology is another double-edged sword that can either heal or hurt, depending on how the technology is managed. Concerns about use of bio-weapons and biological warfare are high. Since the late 1970s there has been a surge of investment in biotechnology research that will not only lead to medical advances but also make it possible to introduce genetic changes to food crops to bring about higher yields and better resistance to disease. The combination of IT and biotechnology has allowed substantial genome sequencing and analysis, creating a wealth of information in the areas of healthcare, food production and agriculture. While so many benefits are brought forth by advances in the life sciences, greater understanding of processes that underpin life raises several moral and ethical concerns about biological warfare. Combination of biotechnology and nanotechnology in future may help in realisation of unprecedented miniaturisation and new capabilities that could be used for both constructive as well as destructive purposes.

Another area of potential impact is energy technology. Future possibilities could include an alternative cheap and abundant source of energy that would

not only revolutionise everyday life, but also shift the strategic balance of oil-dependent economies. Research on controlled thermonuclear fusion could provide unlimited energy from sea-water. Similarly, future research on hydrogen fuel may revolutionise the automobile industry and propulsion technologies. This cutting-edge research work would also facilitate the realisation of practical, affordable energy weapons that could totally revolutionise conventional warfare and alter security perceptions due to introduction of new dimensions to threat perceptions. These examples are only a few sample possibilities. Several such technologies that could create opportunities for quantum leaps in techno-military capabilities are bound to affect the future.

This chapter attempts an appreciation of the interplay of technology with security and international affairs, and also presents a brief review of the S&T strength of India today, in the context of how this could be leveraged for influencing I.R. in furthering India's national interests. Modern Information-Communication-Technology (ICT) can combine world-wide information and knowledge for promoting universal good and addressing common concerns of future global society. India must have a major international role in this new knowledge-based society that will pose many new challenges for diplomacy and I.R.

Technology and Security: Challenges for India

I.R. in the globalised world is going through a major transition phase, where evolving political, economic, social and technological developments are converging to shape a 'New World Order'. In the emerging international landscape, powerful techno-commercial entities and non-governmental organisations (NGOs) that are linked electronically across national borders are creating a new global civil society influencing governments and promoting adherence to principles of social justice and democratisation. The 'State' here is becoming one among many actors, but remains responsible for tracking the larger picture and setting the diplomatic agenda for I.R. The rapidly changing environment of this 'Globalising Age' thus poses new challenges for the manner in which diplomacy will be perceived and conducted in future.

Perceptions of national security are changing in the backdrop of major techno-economic challenges facing the world today that are of global dimension, like global energy shortages and global warming and its consequences on climate. Humanity has entered an 'age of consequences' where the actions or non-actions of the present generation will have profound

impact on future generations. In this emerging 'New World Order', competition and cooperation must co-exist to serve the common good. Understanding of the new realities of this technology-driven economic globalisation will be very important for defining the new role for diplomacy in the future.

It is at this tumultuous time that India is emerging as a potential world-class power and what India does or does not do, is now closely observed by other nations. The main challenge for policy experts in the country will be to make India achieve the power status commensurate with its real techno-economic strength, as quickly as possible, in the multi-polar international equations, where new opportunities as well as new concerns will define the future dynamics. It is therefore, imperative for India to recognise the vital linkages between foreign policy, defence strategy and the economic agenda with the S&T strength of the country. This would help in evolving an integrated national strategy that can best leverage the hard power of techno-military superiority combined with the soft power of diplomacy, trade, education and cultural equations, to serve the larger goals of national interest. Technology has been the major driver of change in modern society and will continue to be so in the foreseeable future. Hence, the impact of future technology advances on security perceptions and international affairs deserves a clear understanding by those representing India at various international forums. The ultimate objective of foreign policy and diplomacy is to protect one's national priorities in the international arena.

The impact of technology on security has been increasing steadily over the past several decades since World War II with several impressive advances in modern technologies reaching maturity. Almost all modern technology advances have been driven by the need for techno-military superiority over other nations and the emphasis is now shifting more towards techno-economic superiority. The two most striking technology milestones of the 20th century that profoundly affected I.R. were the advent of NW and the start of space explorations. These two have transformed the international discourse on security and foreign policy for most major nations in the world, as was evident in the race for superior technology by the two superpowers locked in cold war rivalry for over four decades.

These decades therefore, witnessed phenomenal growth in technology for both military and civilian applications when, it was largely the military strategists who called for superior technology and weapons to remain ahead of the enemy. Scientific inventions and technological innovations have always

been motivated by national security perceptions and foreign policy goals. It is well known that almost everything that the National Aeronautics and Space Administration (NASA), US has ever done in space or high technology has been predominantly motivated by the security perspective. Whether it is the miniaturisation in electronics, achieved through very large-scale integration (VLSI) techniques, or high-sensitivity video camera technology for satellite imaging, most high-tech developments were driven by the cold war's security imperative to maintain the technological edge over the adversary, so that bilateral diplomatic negotiations could be conducted from a position of strength. It was a constant race of technological catch-up, where, often other priorities of economics and development got short-changed in the non-democratic Soviet empire and the mighty Soviet Union paid the price with its economic collapse and the disintegration that followed.

For the US this was the period of unprecedented growth in technology capabilities both in defence and development because of its prudent use of dual-use technology for simultaneously energizing the economy, and enhancing defence capabilities. Countries that could not politically manage the rapid change or did not have the technology strength struggled to keep moving forward lest they be left far behind. Perceptions of national strength shifted gradually but completely, towards techno-economic strength, as against the earlier perceptions that vast armies and massive war-fighting equipment represented true strength. Other nations on the technology-acquisition path have a lot to learn from this US model because it imposed a heavy economic burden on the adversary and this contributed to weakening or defeating the latter. This victory did not involve fighting a war, a significant achievement given the history of mankind. Techno-economic competition therefore, stands proven as one of the most effective tools for defeating a political or military adversary.

The US victory over the Soviet Union was however, not without problems. Many new technology-related security concerns emerged from the disintegration of the Soviet Union. Of major concern was the safety of the large stockpile of NW and fissile materials. The stockpiles of the two then superpowers exceeded the limits of economic viability and safety management, and some initiatives for mutual disarmament were already in progress even before 1990. This provided some background and familiarity with the issues of rapid disarmament and related safety issues. However, the progress of the major disarmament agreement, Strategic Arms Reduction Treaty (START) leaves much to be desired.[4]

Technology diffusion may be defined as the natural spread of technology through every type of technology interaction, whether acquisition, development, transfer, co-production or even intellectual exchange. A major problem after the break-up of the Soviet Union was the vast bank of knowledge invested in Soviet scientists, who lost their privileged access to State resources at a time when political changes made it easier for them to establish connections with foreign potential buyers of their expertise. The risk that this knowledge would spread according to the logic of market forces led the US to initiate a major project to absorb and rehabilitate these scientists. Other countries such as China and Israel also used the opportunity to their advantage. The importance of technological knowledge for security was again vividly demonstrated. The ubiquitous nature of technological knowledge is largely responsible for technology diffusion in intangible ways that are not easily obvious to monitoring and control agencies and this contributes invisibly to the process of technology diffusion.

It is interesting to note that while the West was occupied with the management of dangers related to the catastrophic failure of the Soviet system, China was quick to learn from immediate history and used the so-called peace dividend to maximum advantage. China reviewed its military modernisation efforts, under way since the 1980s and chose to concentrate fully on re-orienting it for techno-industrial superiority to match the best in the world and on building economic competitiveness to overtake its powerful neighbour, Japan. Throughout the 1990s, China continued on its path of rapid economic growth and consolidated its military and commercial technology base. The rise of China as a potential world power is largely due to the vision of its leaders, who pushed the country for impressive growth in its manufacturing base, to gain a globally competitive edge that in turn helped it to emerge as the most powerful nation second only to the US. The 21st century has begun with many changed parameters relating to technological options for defence and security, where issues of access to sensitive technology and use of modern lethal weapon technology have become important concerns for I.R. and diplomacy. While the military operation in Iraq will remain a major milestone of the 21st century—where the US was in the driver's seat, the other equally unforgettable event of this young century was the 9/11 event, that saw the US under attack in its own homeland by extremists with relatively modest technology capability.

Terrorist networks have learned how to exploit high-tech mechanisms such as the internet and global banking systems to raise funds, plan, coordinate

and communicate. The menace is no longer confined to small, disgruntled religious fanatic groups but has acquired a ubiquitous global presence. Extremism has been fuelled and funded by short-sighted leaders or dictatorial State actors that want to use these elements for their military and diplomatic advantage. Given the scale of operations of terrorist organisations it should be easy to understand that such non-state terrorist groups could not have gained this amorphous global presence without State-level support.

Nevertheless, it is not the technology *per se* that is good or bad, rather its application, with dangerous intentions or irresponsible attitudes that is the real cause for concern. If used properly and in a balanced manner, technology is an invaluable key to security, development, progress, cooperation and harmony. The future challenge therefore, will be to facilitate best use of technology for all mankind, to allow universal progress, peace and stability, while managing technology interactions and technology advances in a way to prevent its careless misuse or dangerous abuse. This can best happen when all stake-holders in modern society learn to respect S&T and remain committed to using technology prudently for the common good for all mankind.

As long as nations continue to be unequal in economic wealth and techno-military power or have differences on ideological, religious or cultural grounds, their relationships will be uneven and problematic. Convergence of views and interests can emerge only in areas where there are common fears or mutual benefits. Progress, peace and stability are major goals that are shared worldwide. Technology is often the common denominator that can help bridge some of the avoidable gaps and thus play an important levelling role, to enhance international cooperation for long-term benefits for all humanity. Fortunately, among the progressive nations, now there is a far better appreciation of the effects of technological advances as well as better techno-political maturity in using technology for security needs, economic development, social progress and political leverage. Thus, the changing global security scenario presents a unique opportunity to foreign policy experts and diplomats to use technology as a binding force to build a safer, progressive and peaceful world society.

As is well known, the modern concepts for technology control were driven by the need to arrest proliferation of NW and its devastating effects. With increasing potential of technology for mass destruction or mass disruption, reducing the threat of potentially dangerous technologies and weapons, as well as controlling the possible misuse of dual-use technologies will remain the major challenges for international non-proliferation efforts and the

technology-control architecture of the future. In the past, under the presumption that sensitive technologies are safe within the country or group of friendly allies, technology controls became synonymous with export controls of critical commodities or systems. But now, controlling the know-how and knowledge has become increasingly important and in future, diffusion of knowledge will become inevitable in the globalising world. Hence, controlling or managing human intentions will emerge as the main challenge of the future for preventing misuse of potentially dangerous technology.

Changing patterns of economic progress, global market forces, technology diffusion and new security perceptions will require a radically fresh approach to the effective management of technology in the 21st century. Rise of religious fundamentalism and ready availability of mercenary non-state forces, has added a new dimension of asymmetric threat, and it is imperative that dual-use modern technology access to such extremist groups must be prevented without bias or subjectivity. At the same time, cooperation and interdependence among peace loving nations is becoming increasingly essential for combating such a ubiquitous threat and in this case too, international technology co-operation alone will be the main vehicle to evolve effective solutions.

Hence, the challenge will be to manage the dynamic balance of technology control with the imperatives of cooperation and healthy competition between nations. The solutions for the future must therefore be evolved imaginatively, based on mature and informed management of international relations for national or regional security. Foreign policy experts and diplomats of the future thus, must have the appropriate knowledge-base to understand the finer nuances of modern dual-use technology, to develop informed negotiating strategies for international dialogue and diplomacy in the future.

Indian Perspective

During the two centuries of British Raj the main focus was maximum exploitation of India's resources for the benefit of the ruling empire and little was done for the development of the land or its people. Hence, India after independence in 1947 had to concentrate on nation-building and human development. Compulsions of the cold war years saw India becoming alienated from the advancing Western alliance and more dependent on cooperation with the USSR. This led to India being labelled as a Soviet bloc nation and a target country for technology denial by the Western group of countries. The situation got worse after the 1974 'Peaceful Nuclear Experiment' (PNE) by India to create a notional deterrence against nuclear China. As already discussed in

the previous chapter, the Nuclear Suppliers Group (NSG) was formed to tighten the technology controls of all dual-use items that could contribute to nuclear R&D. The next step was the establishment of a seven nation group in 1983 to control ballistic missile development through the MTCR that created further discrimination and hence, it was not very successful.

By that time, India had already embarked on major defence system projects such as the Main Battle Tank (MBT), the Light Combat Aircraft (LCA) and the IGMDP (Integrated Guided Missile Development Programme) in its efforts towards enhancing self-reliance in defence technology and these projects were facing very tight export controls for basic materials and components. It was in this context, that at a high level meeting between the Indian Ministry of Defence (MoD) and the office of the US Secretary of Defense, a diplomatic agreement was worked out to appoint a Defence Adviser in each country to build confidence on both sides, to enable the US defense industry to gain from significant business opportunity in India. India readily agreed to this arrangement as it could lead to softening of technology denials for some critical items that India needed urgently for important projects.

The process started in 1988-89 with understanding the actual US concerns on dual-use technology and custom-tailoring the Indian requests for items and sub-systems to fit within the limits of US acceptability, with a mutually evolved 'End Use Certification' process. Personal contacts developed with officials at the Pentagon, the US Air Force, the State Department and the Commerce Department proved very useful for engaging US officials in constructive dialogue, for defining mutually acceptable specifications and limits of usage.

Starting with the successful contract for supply of General Electric (GE) engines for the LCA, the list of previously denied systems and components in avionics and sensors for removal of denials, slowly increased to impressive numbers during the six-year tenure of the first Adviser, Defence Technology at Washington DC. The US defense industry leaders emerged as the main supporters of the Indian initiative as they were keen to expand their overseas business through the emerging new Indo-US technology cooperation.[5]

The presence of a defence technology expert at the Indian Embassy at Washington was uniquely beneficial to foreign service officers of the embassy in enhancing their own appreciation of technological nuances, while for the Defence Adviser, the experience was equally rewarding in understanding the finer aspects of foreign policy practice. Working level contacts within the US

Government system and increasing mutual familiarity, helped in building mutual confidence of dependable equations for contracts worth millions of dollars, which would otherwise be denied to India. Collapse of the Soviet Union and end of the cold war also helped in opening up new possibilities of Indo-US cooperation, and joint working groups were formed to further strengthen the techno-political equations. Indian foreign service officers and the US State Department officials played an important role in their respective governments to leverage the growing technology cooperation for strategic partnership. The seeds of the US-India "NSSP" (Next Steps in Strategic Partnership) were thus sowed in the early 1990s.

It must be put on record here that two other factors played major roles in changing the international perception of India. The first was the economic reforms of 1991 that immediately mobilised the market forces to attract investments into India; the second was the IT revolution around the turn of the century, where the Indian technology workforce made global headlines for contributing to the global transformation to digital technology. The technology content of both these factors was very significant and India could benefit from this transformation only because the country was mature enough to leverage its technology and intellectual strengths. Political overtones of these changes were very deep and signalled India's arrival at the global stage as a major techno-economic player.

Future Trends in Technology and Security Strategy

The past decade has been one of introspection and self-evaluation for many progressive nations, giving them occasion to assess their existing potential and identify future priority areas for enhancing their security and stability. The results have represented something of a military-technical revolution throughout the world, albeit at different levels of sophistication. The strategic focus during the cold war period was on countering the capabilities of the adversary with technological innovations. This also implied denying the adversary the advantages of technology as much as possible. Based on major military platforms and weapon systems, the strategy was to constantly improve performance and enlarge the inventory. Although this type of focus continues to be relevant in the context of some regional conflict scenarios, for most militarily advanced nations the focus is now clearly shifting to strategies based on a 'system of systems' approach.

Technological maturity and the compatibility of various systems have made it possible to plan for enhanced military capabilities, based on a

combination of individual technologies. For instance, one major trend indicates a preference for the integration of long-range, high-precision weapons, which rely heavily on satellite-based reconnaissance and advanced sensors with the use of fast digital communication links. Another trend indicates the use of sophisticated airborne or shipboard platforms with customised targeting techniques and a variety of warhead options for intended application objectives.

Another important strategic shift that has occurred is the increased focus on C^3I technologies (Command-Control-Communication-Intelligence) for conducting integrated war operations with quick reaction time and maximum flexibility. The ongoing revolution in IT has enabled vast arrays of advanced sensors to be used simultaneously for gathering intelligence and for decision support systems. Compact and fast computers have transformed the battlefield and it is now possible for an individual soldier to possess high situational awareness in real time. With such advanced technological capabilities, older war-fighting doctrines will clearly be replaced by new tailor-made flexible strategies that can allow optimal use of military assets under any given circumstances.

Yet another important contribution of technology to future strategic planning is the availability of advanced simulation and war-gaming capabilities. These not only allow major improvements in planning but also help to evaluate the effectiveness of various options for defence strategists and planners. Simulators are also invaluable for high-level training for complex weapon systems. The higher the level of technological sophistication, the higher the demand for comprehensive training without which high-tech equipment becomes practically useless. Future military strategies will need to take into account some important technology trends. First, the role of dual-use technologies will be far more relevant, with many military capabilities based on civilian technologies. This means that more countries will have access to military capabilities that were available only to a few powers in the past. In a sense, this means that the technology gap between the most advanced and the average-level countries will be reduced overall.

Hence, strategies and tactics need to ensure that available technology will play a larger role in the future. Given shrinking defence budgets, reduced or changed threat perceptions and acute economic competition, defence producers will tend to change their business practices to make more technological options available to partners and customers in a large number of nations or groups. This increases the potential for asymmetric conflict situations and the use of low-intensity warfare techniques. In the regional

context, the implications can seriously influence security concerns and military strategies. Export controls and arms control in such situations become increasingly difficult to implement and a sense of lack of control can, in turn, only further fuel the proliferation of conventional weapon technologies. In the regional context, therefore, the trend will be to counter the techno-military capabilities of immediate adversaries, in a way that may not be directly related to the technology revolution taking place in the developed world. The regional dynamics of the interplay between strategy and technology will be different in different cases.

Despite the increasing diffusion of technology in many fields, the technology gap will probably remain at the same level or even grow, because of the sheer cost and complexity of sophisticated technologies. Stealth technology, smart weapons, Intercontinental Ballistic Missiles (ICBMs), strategic cruise missiles and nuclear submarines are examples of technologies that will remain restricted to only a few nations that have the techno-economic means and maturity to possess and use them. Hence, when new technological capabilities are added in future by a technology leader such as the US, few other countries may have either the means or the motivation to invest heavily in countering them. The strategies of the target countries may therefore shift towards the acquisition of asymmetric advantages from WMD, or they may resort to low-technology counter-measures such as developing assets underground for protection. These are some of the interesting aspects of technology interplay in the security strategies of the future.

The current military technology transformation is being led by advances in the US, where the focus is clearly on using IT and space technology for maximum techno-military advantage. The 2003 military operation in Iraq was a convincing demonstration of the new strategy of Network-Centric Warfare (NCW). It is obvious that for the past decade, US planners have redefined their strategic priorities to reflect a mission-oriented strategy, rather than the previous finite goal of fighting two parallel simultaneous wars, as enumerated in military doctrines towards the end of the cold war. The US concept of military transformation envisages the full spectrum of technology enhancement and the introduction of new technologies and capabilities to maximum advantage. Rather than defining an end objective, the strategy appears to be largely evolutionary, allowing for constant change and flexibility. The decision to pull out of the Anti-Ballistic Missile (ABM) Treaty and to deploy a Ballistic Missile Defence (BMD) system clearly signals the US' preference for a unilateral approach—with a renewed focus on homeland

security—to global issues such as countering terrorism or controlling WMD proliferation. However, even the US cannot afford to ignore the importance of cooperative security management and multilateral approaches.

In technology terms, new and emerging dimensions of security and threat perceptions must include the security of outer space and space assets on the one hand, and the real threat to information security, on the other. Protecting information in cyber space is already proving to be a major challenge. The vulnerability of information-dependent modern societies to information warfare makes this an urgent issue. International norms or formal treaties on these new technology aspects are yet to evolve adequately and the potential for cyber terrorism remains a real time threat to military systems as well as to civil infrastructure such as financial institutions, power-supply systems and air traffic controls. The ubiquitous nature of cyber space makes information warfare a potential tool for control, as well as threat. The counter-countermeasure race in IT may not be visible, but will certainly spur rapid growth in technological capabilities. The subject of weapons in space, however, is one of high visibility and could transform strategic thinking around the world. If it leads to accentuated insecurity for a larger group of nations, this will be a sad commentary on technological miscalculation of the century at the global level.

The nature of nuclear deterrence has undergone a change because some of the modern advances in conventional weapon technologies have led to such powerful capabilities that the deterrence value of these advanced weapons has improved substantially. In future, the 'system of systems' approach, combining the potential advantages of several high-tech military capabilities, may even provide deterrence comparable to nuclear deterrence, largely because of its international acceptability and the ready usability of these weapons. The international community is already committed to a total ban on Chemical and Biological Warfare (CBW). Effective implementation of the BTWC (Biological and Toxin Weapons Convention) and the CWC (Chemical Weapons Convention) could enhance CBW to zero deterrence level. The extreme asymmetric technique of using terrorism as a means to achieve political–military objectives is also close to being universally unacceptable. Hence, there is hope for reduced dependence on NW for deterrence by major powers and potential for an eventual international agreement on universal nuclear disarmament.

The major issue that future technology control mechanisms will need to address is that of rapid technology diffusion. This is true for several reasons.

Technology advances are very fast and spread across a wide spectrum of disciplines. Globalisation, as well as unprecedented global transparency as a consequence of instant worldwide media coverage, has transformed technological awareness all over the world. A poor villager in a remote area of a developing country is today more aware of world events and of what the richest in the world can afford. It is this awareness that is the most powerful driver for a large part of the world's population to seek technology access and related opportunities for progress. The have-nots of yesterday did not fully realise what they did not have. In the 21st century, such awareness is much more acute and often keeps pace with global developments. In the high-technology sector, industrial practices are constantly changing to remain competitive. In the emerging new technology domain, it is increasingly difficult to define the line between civilian use of technologies and potential dual-use technologies. Innovation is the buzzword and there are several intra-industry information sharing arrangements across international borders, set up for purely commercial reasons that defy external controls.

A new dimension of export control problems is the increasing importance of the individual's personal technological knowledge. In sensitive high-technology areas such as nuclear science, propulsion and guidance technologies, simulation techniques, micro-miniaturisation, electronic design and laser technologies, it takes years of first-hand experience to develop expertise. The past five decades have seen a gradual rise of such expertise, not just in the Western group of supplier countries, but all over the world. These experts are the real repositories of technological knowledge, and they certainly cannot be subjected to typical export control procedures. Similarly, the technological capabilities of a nation depend significantly on its industrial infrastructure and a certain techno-industrial culture that develops over time, with techno-economic progress. These are not physical commodities or services that can be controlled through export, unless export controls are made so restrictive as to deny a country every kind of information on processes and technology. This approach would border on sanction-like measures that are normally used only as punitive actions.

The 21st century situation is thus unlike the 1950s–1990s, when the majority of technologies were being developed under the umbrella of military–industrial complexes of the two superpowers, and the situation is continuing to change fairly rapidly. Increasingly, technology is being developed largely by civilian sector enterprises and multinational companies that cut across the globe and work primarily for economic development and commercial benefits.

In the age of globalisation, it would be economically impractical for each nation to seek to develop the whole spectrum of indigenous technology infrastructure. However, given the interplay of sensitive technologies in ever changing international security calculations, it is important for progressive nations to develop core competences in critical and sensitive technology areas. Only countries that have the basic scientific and technological infrastructure and maturity can really absorb high technology and thus, benefit from the processes of technology diffusion around the world.

Technological know-how is now increasingly held by private companies that are suppliers to their own governments as well as to others, through exports. Apart from military products, ordnance and ammunition which continue to be controlled largely by governmental agencies, most high-technology components and sub-systems are now dual-use in a reverse mode—that is, it is now civilian technology advances that are creating newer military applications. This process started even before the end of the cold war, and arms control negotiators even then had to decide what to control and how. Almost everything today is dual-use except for weapon-grade fissile material and some biological precursors that are potential ingredients only for WMD—extreme examples of technologies that are unlikely to be commonplace. Across the wide application spectrum of technologies for aeronautics, electronics, propulsion, guidance, sensors or digital electronics, it is difficult to separate out what may be of exclusive military use and hence, a clear candidate for control regimes. These cutting-edge technologies are now held mostly by commercial companies, where technology is more often knowledge-based than defined merely in terms of components and hardware.

A major factor behind technological diffusion is the potential for high technology to command the highest price in the commercial marketplace. Most industrially advanced nations depend heavily on export earnings to remain economically competitive and therefore are subject to forces of competition. These drivers for technology diffusion will always work against the efforts for technology control and export regulation. Regional and global security will demand a delicate balance of these technology-oriented interactions towards protecting security concerns, without seriously hampering the course of regional economics and international trade. In the global economy no company can be competitive without successful exports and yet, when it comes to the costs of adhering to export controls, it is usually companies rather than governments that pay.

Large companies are acquiring other smaller companies and mergers are

being worked out across the world between partners that were previously rivals. High-tech companies and defence industries are particularly hard-pressed to survive and strongly resent the overbearing export control regulations that restrict their ability to innovate and move ahead in global competition. These companies have to move at real-time speed and cannot tolerate the bureaucratic or legalistic delays of export control regimes. The nature of threats to security and stability has undergone a sea change and most modern technological capabilities are beginning to appear as double-edged swords. Who could have imagined that commercial aircraft could be used to cause such devastation and death as was brought about by the terrorists who carried out the attack on September 11, 2001!

Another dimension to technological change arises from changes in the way in which technology is inducted into the military domain. In the majority of technologies that have the potential to influence military capabilities, civilian R&D is now often in the lead. Earlier, it was military technology that was driving civilian industrial development and the military was the first to take advantage of new technologies, and thereby control the civilian adaptation of these technologies. In the 21st century, civilian R&D is often ahead in most new technology areas. In future, military applications may actually follow after civilian adaptation because induction of technological innovation into military systems is a long process fraught with innumerable and complex considerations of integration, inter-operability and cost-effectiveness. Drivers for civilian adaptation are indeed very different.

Private sector R&D can no longer afford to be hampered by bureaucratic and security restrictions and is, thus, racing ahead with faster innovations, better flexibilities and more competitive management infrastructures. This trend will become even sharper in the future and the whole system of technology induction into the military and security apparatus will undergo a sea change. Future technology control regimes will have to adjust quickly to these sweeping changes. Controlling exports of emerging dual-use technologies is going to become far more challenging. Decades of technology denial has spurred indigenous R&D in many progressive developing nations and traditional target States such as China and India, are becoming important economic and military powers. Several developing nations have emerged as attractive markets for high-technology products. Since these countries are not participants in the 'supply club', there is some concern that the situation may lead to secondary proliferation of sensitive dual-use technologies, given the futility of denying what already exists. It is interesting to note that although

both China and India have voluntarily established and updated their export control regulations to match international standards, they have not joined any supply cartel for technology controls.

Western supplier groups still have difficulty accepting them as partners, whereas some of the former Soviet republics with fledgling economies and doubtful infrastructure for export controls have been welcomed as partners for the future. The issues, however, are even more complex. The progressive developing nations today have become smart buyers that insist on technology transfer with every procurement interaction. High technology is a buyers' market today, so it is difficult for the supplier to refuse such deals for fear of being beaten by the competition. The effect is that the technology gap between the industrially advanced countries and the developing countries is becoming smaller with time. Except for the US, which has relentlessly continued with high-tech R&D and innovation, most other participants in the multilateral export control regimes stand to lose some of their technological edge and with it, the high ground for export controls. The US in turn, may then justifiably look for ways and means to maintain its superiority, by exercising unilateral controls against the rest of the world, including some of its former allies, through a unilateral export control regime.

The special feature of modern technology is the high relevance of intangible transfers, through the exchange of scientific information among experts. Excessive or intrusive controls, such as attempts to control intangible technology transfers through monitoring normal scientific–technical relations among experts should be avoided, because they would be counter-productive to the larger goal of wider international cooperation. These are some of the finer nuances of the technology diffusion and technology transfer challenge that must be borne in mind, when trying to fine-tune the technology controls of the future.

Indian Science and Technology Potential for Influencing International Relations

India has taken major strides in science and technology since its independence and is recognised today for its achievements in many fields ranging from agriculture, textiles, healthcare and pharmaceuticals to info-tech, biotechnology, space technology, and nuclear technology. All this, combined with India's role in the global IT revolution, as well as India's indigenous strength in many key areas of defence and strategic technologies, has made

India a significant player on the world stage. Quite appropriately, Indian foreign policy has also undergone a silent reform and India today is seen as a responsible and stable democracy with a major role in regional and world power equations. The US signing the civil nuclear technology cooperation agreement with India, within ten years of announcing sanctions against India's nuclear tests in May 1998, speaks volumes of this remarkable transformation it has achieved through its combined maturity in technology and diplomacy.

At the onset of independence, India's first Prime Minister, Pandit Jawaharlal Nehru called science 'the very texture of life and optimistically declared that, 'Science alone can solve problems of hunger and poverty, sanitation and illiteracy, as well as problems of superstition and retrograde customs.' Under his leadership, first the Indian Government set out to cure numerous societal problems. The Department of Atomic Energy, the Department of Science and Technology and the Department of Space were among the first S&T departments in the country of which, the Prime Minister himself took charge. The Green Revolution, educational improvement, establishment of hundreds of scientific laboratories, industrial and military research, massive hydroelectric projects, and entry into the frontiers of space—all evolved from this early vision to embrace high technology.

Indian scientific research and technological developments since independence in 1947, have received robust political support throughout, and almost all the initial funding has come from the government. Science and technology initiatives have been important aspects of the government's Five-Year Plans and are usually focused on fulfilling short-term needs, while aiming to provide the institutional base needed to achieve long-term goals. As India set out to empower leading scientists to create world-class research institutions, government-sponsored scientific and technical developments have aided diverse areas such as agriculture, biotechnology, high altitude and oceanographic research, communications and entertainment technology, energy technologies, mining, nuclear power, space, defence and transportation etc.

Soon after independence, the government took several initiatives to set up a number of policy-level bodies to promote S&T in the country. The Scientific Advisory Committee to the Cabinet (SACC) was set up in 1956 and an improved Committee on Science and Technology (COST) was established in 1968. A National Committee on Science and Technology (NCST) was established in 1971 to formulate and continuously update comprehensive S&T plans. The first S&T plan formulated by NCST

identified 24 major sectors for priority S&T development and laid as much emphasis on the development of engineering, design, and fabrication skills as on the development of technology. The SACC was restored in 1981. In addition, there is a Cabinet Committee on Science and Technology. The National Council of Science and Technology is the apex body chaired by the prime minister, and the integration of S&T planning with national socio-economic planning, is the responsibility of the Planning Commission, now replaced by 'Niti Aayog'.

The post-independence era also saw the setting up of the five IITs, starting with Kharagpur in 1950, Bombay in 1958, Madras in 1959, Kanpur in 1960 and IIT, Delhi in 1961, all quite unique and recognised for world-class standards. A new Ministry of Science and Technology was established in 1971 and several national laboratories got re-organised under the Department of Science and Technology (DST) and the Department of Scientific and Industrial Research (DSIR) that also includes the CSIR (Council of Scientific and Industrial Research) laboratories. Meanwhile, the Department of Atomic Energy, Department of Space and the Department of Defence R&D also evolved, with many laboratories getting set-up in key critical technology areas.

These premier R&D institutions, some leading universities and the string of national level laboratories today represent the backbone of Indian S&T. Against this backdrop, one would expect India to be much organised in S&T issues and a very high achiever in all aspects. However, shadowed by the compulsions of a developing country, Indian S&T policies were focused on mission mode projects of national importance; and most achievements of independent India are of the type where successful application of already known technology was done by government agencies or institutions. While this can be seen as a success of the S&T policy, unfortunately it also resulted in the decline of open-ended basic research of excellence, except for some pockets of excellence. Overall, there has been a fall in scientific research output, both in quantity and quality, because of sub-optimal resourcing and short-sighted goals of the scientific and engineering community. In the first five decades since independence, India had to concentrate on survival and sustainability; now India must aim to rise rapidly in world S&T competition and establish itself as a technology leader in select areas of high priority. Some of this is indeed happening, but the pace needs to be faster.

Science and Technology Policy Framework

Science and technology development in India owes a lot to a series of policy

instruments enunciated by the Parliament, such as the 'Scientific Policy Resolution' (SPR) of 1958, which emphasises the government's responsibility to foster, promote and sustain the cultivation of science and scientific research in all its aspects of pure, applied and educational. The key role of technology as an element of national development is also well recognised. The Department of Science and Technology has been formulating policy statements and guidelines on S&T that provide a vision for institutions involved in different areas of S&T to work towards the common goal of furthering the cause of S&T in India. S&T policy documents have evolved with changing times and priorities of the nation and they state the principles on which the growth of science and technology in India has been based, over the past several decades.

One of the early planning documents was the SPR, which called for embracing 'by all appropriate means, the cultivation of science research in all its aspects—pure, applied and educational' and encouraged individual initiatives. In 1983, the government issued a similar statement laying considerable emphasis on self-reliance and development of indigenous technologies, while also stressing the importance of international cooperation and diffusion of scientific knowledge. The Science and Technology Policy of 2001 addressed the need for restructuring the administrative and management structures associated with government science departments, agencies and many institutions. The latest revision to the Science and Technology Policy in 2003, once again, emphasises the goals of self-reliance and adds focus on sustainable development and equitable distribution for the country.[6]

The government evolved certain instruments for the implementation of technology policies in 2001, which were also applied to the technology policy of 2003. The priority areas and their strategies for implementation were broadly identified, and due recognition was accorded to the importance of knowledge-based development and competition, to meet national needs in the new era of globalisation. Sensitivities to Intellectual Property Rights (IPR) issues and the compulsions of international cooperation are new additional dimensions of the emerging S&T scene.

Technology Development in India

History has shown that modern economic growth has been inspired by a rapid and persistent upgradation of technology and scientific know-how. It is estimated that from one-third to one-half of the growth experienced by the industrially advanced countries has come from technological progress. Thus, technology has emerged as the principal driving force for long-term economic

growth. Economic growth results both from slow and steady improvements in technology and from knowledge embodied in physical and human capital as well as from the "breakthrough" inventions.

Post-independence, the national leaders of India adopted a socialist view to industrialisation and three of the main aspects that emerged from their policies were: (a) government intervention and control: government monopoly over industries, nationalisation of banks, extensive and influential public sector (b) neglect of exports and (c) economic development giving direction to technology development.

At the time of independence in India, industrialisation was viewed as the engine of growth for the rest of the economy and the supplier of jobs to reduce poverty. However, industrial production rose only marginally till the 1970s. Compulsions of other societal developments and the emphasis on large-scale, capital-intensive industries created far fewer jobs than the estimated ten million annual entrants into the labour force required. Hence, unemployment and underemployment remained growing problems. In the 1990s however, industrial production rose at an average rate of 6.6 percent. Observers believed that this increase was largely a response to economic liberalisation, which led to increased investment and competition. By the mid-1990s, substantial progress was made but industrial growth still failed to live up to the expectations.

The new government gave top priority to economic planning for development. Steps were taken to accelerate industrialisation and redress regional imbalances. Progress was slow, as the infrastructure was not there. People had very high expectations and the government had to provide for education, healthcare and employment for hundreds of millions of people. For more than three decades, India's national income grew by no more than 3.6 percent a year, one of the slowest growth rates in the developing world. Its per capita income was among the lowest.

The thrust on S&T continued during Indira Gandhi's premiership, including the Pokhran I series of nuclear explosions in 1974. In subsequent years, India became host to one of the two International Centres for Genetic Engineering and Biotechnology (ICGEB). Prime Minister Rajiv Gandhi also provided strong political support to science and technology, including ICT.

It took the nation almost half a century to find its feet. Today, India is a nuclear power and has launched its own satellites into space; it produces its own steel and builds its own warships and many critical parts of its aircraft.

It has an impressive heavy engineering base and is one of the few developing countries that have been able to bid successfully for heavy engineering turnkey contracts in other developing countries. Its progress in agriculture is equally impressive. The driving force behind India's S&T came from government initiatives such as those in atomic energy, space, and biotechnology. Fortunately, in recent years, the private sector has emerged as the driver in areas such as information technology, biotechnology, the pharmaceutical industry and the automobile industry. The transition is a continuing phase, with some Indian industries attaining global dimensions and competing with the very best in the world.

The IT industry in India is one of the fastest growing industries. The Indian IT industry has built up valuable brand equity for itself in global markets. The IT industry in India comprises the software industry and information technology-enabled services (ITES), which also includes the business process outsourcing (BPO) industry. India is considered a pioneer in software development and a favourite destination for IT-enabled services. The industry has not only transformed India's image on the global platform, but also fuelled economic growth by energising the higher education sector, especially in engineering and computer science. The industry has employed almost ten million Indians and has contributed a lot to social transformation in the country.

Government policy towards the IT sector changed when Rajiv Gandhi became Prime Minister in 1984. His New Computer Policy (NCP-1984) consisted of a package of reduced import tariffs on hardware and software (reduced to 60 percent). Some of the policy reforms included de-licensing of the software industry for exports, so that it could be eligible for bank finance and freed from license-permit raj and permission for foreign firms to set up wholly-owned, export-dedicated IT industry units. A special project was initiated to set up a chain of software parks in India which could offer infrastructure at below-market costs. These policies laid the foundation for the development of a world-class IT industry in India. Today, Indian IT companies such as Tata Consultancy Services (TCS), Wipro, Infosys, and Hindustan Computers Ltd. (HCL) etc. are renowned in the global market for their IT prowess. Interestingly, the majority of these are private sector holdings.

The Indian education system places strong emphasis on mathematics and science resulting in a large number of science and engineering graduates. Mastery over quantitative concepts coupled with English proficiency, has

resulted in a skill set that has enabled India to reap the benefits of the current international demand for IT. Also, the cost of software development and other services in India is very competitive as compared to the West. The S&T infrastructure in India today is fairly wide, encompassing all S&T organisations under the central government, state governments as well as public sector entities, working in areas as diverse as agriculture, healthcare, industrial development as well as nuclear, space and cyber space R&D. Significant contributors are the large number of institutes/undertakings functioning under the central government S&T departments and the trained personnel employed by them, rightfully making them India's S&T assets.

For India to really become dominant in technology and innovation, what is required is an innovation ecosystem that links markets, companies, R&D centres and venture capitalists. India must have a proactive approach that is not risk-averse and policy reforms that can attract and utilise the best talent. China is a good case-study of how a well-planned approach to technology development and innovation over 2–3 decades has enabled a country to compete with the best in the world. India also needs a pre-planned and aggressive approach to technology planning, development, acquisition and innovation. The R&D component in Indian industries has been very minimal and this needs to be enhanced very effectively through imaginative policy reforms and incentives for small and medium enterprises (SMEs).

Major Initiatives in Indian Science and Technology

The most significant and recent policy level priorities for science and technology in India have come in the form of two major initiatives by the Prime Minister's Office. On March 5, 2005, the cabinet gave in-principal approval to a host of decisions that could have far-reaching implications for science and technology in India. This included setting up of a world-class national science and research foundation and two universities for scientific research and education. First few 'Indian Institute of Science, Education and Research' (IISER) have already started functioning very well in the country. With the 'National Science Foundation' seed money of Rs. 1000 crore, these IISERs would be highly autonomous and would be run by scientists to support establishment of centres of excellence as well as to encourage promising individual scientists. Kolkata and Pune were selected for establishing the new universities at a cost of Rs. 500 crore each, to enhance the status of basic research and also create new opportunities for attractive careers in S&T. The

same cabinet meeting also cleared the launch of three national missions—on scientific literacy, emerging diseases and on safe drinking water.

India's progress over the next 15-20 years will be intimately linked to events within the South Asian region, as well as around the world. Both opportunities and challenges will arise as the result of transformation in the regional and global political and security environment. World trade under the World Trade Organisation (WTO) will determine access to markets and international competitiveness. The economic growth rates of other regions will influence demand for exports and foreign capital flow patterns. Pressures due to rising cost of energy resources, continued spread of information technological innovation, steady increase in world trade—are some other factors that will also impact India's techno-economic progress. The next decade presents a unique opportunity for India to emerge as an S&T leader.

In terms of the impact of globalisation on technology and infrastructure, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) should promote even faster technological innovation around the world. Application and diffusion of technologies in a wide range of disciplines across international borders will accelerate. Agriculture technologies, biotechnology, information technologies and new manufacturing techniques will probably transform how human beings learn, communicate, produce and care for their health.

Many important technology breakthroughs may be expected in areas such as fuel cells, alternative energy, genetic engineering, precision farming, mass communication, computerised healthcare and environmental protection. The cost of global communications will probably continue to decline further, reducing the barriers of distance and bringing new levels of transparent competitiveness in global production, distribution and marketing. In all this, foreign policy needs to be in sync with national S&T priorities and Indian diplomacy must effectively leverage S&T for international objectives.

The next ten years for Indian industry are going to be very different from the last ten years. Increased globalisation, increased choice for customers and employees, increasing competition and new technology inputs will enforce major changes in strategy, for success. Technology development towards its successful commercialisation is a complex process that involves a combination of factors—the choice of technology with correct assessment of market potential, availability of technological competence and financial support, R&D and production support for optimum scale of operation and the infrastructure

and marketing support to make the product competitive. The lack of proper understanding of these complex issues at the policy level has resulted in overall lack of competitive success, except for sporadic success by an individual company.

Towards India's aspirations for technology leadership, it may be worthwhile to make an assessment of its existing strengths and select one or two technologies for scaling-up to international standards in each five-year plan period. Such a scale-up in planning, funding and execution can allow the country as a whole to be recognised as an important player in an increasing number of high-tech areas. This could enable India to become a partner in international S&T mega-missions and perhaps invite talent and funding from across the world for cross fertilisation of knowledge and expertise at an international level.

The present time period represents a unique window of opportunity for international cooperation in high technology. After years of being a target of technology controls, India is finally getting the recognition for its indigenous technology maturity and responsible international conduct. The sheer strength of the knowledge based workforce in India has created a new face for India to qualify as a very important partner in techno-economic affairs of the world. It is imperative that policy makers and administrators take serious note of this historic opportunity and steer the country to new heights in science and technology in the 21st century.

International Relations and Diplomacy in a Globalised World

There has been an interesting shift from traditional and often secret diplomacy of the 20th century to the 'modern diplomacy' of the post-cold war era, to the more recent 'open diplomacy'. The global integration of ICT and increasing use of the world-wide-web has enabled unprecedented dissemination of a variety of information. Information accessibility and transparency has also undergone a sea change. Internet, just about 25 years young in the public domain, is having a profound impact on international affairs. The digital media is a many-to-many type of information technology. From a technology perspective all this has been possible only due to transformations in digital electronics and advances in ultra-fast communication technologies, which is so intrinsic that it is seldom recognised.

The most valuable component of the new media for diplomats is the ability to listen to new audiences and better understand their views and values.

It has led to a new form of statecraft by reshaping diplomatic agendas to meet old challenges in new ways and by deploying innovative approaches to foreign policy reforms. The world today has perhaps what can be defined as e-diplomacy—a new approach which is in addition to all that has been there. This 21st century statecraft complements traditional foreign policy tools with newly innovated and adapted instruments of statecraft that fully leverage the networks, technologies and demographics of our interconnected world. It enables traditional diplomatic services to be delivered faster and more cost-effectively, both to one's own citizens and government and to those of other countries.

Digital Technology in Public Diplomacy

In 2012, the Indian embassy in Cairo, in collaboration with the 'INDIAFRICA' organisation marked the birth anniversary of Mahatma Gandhi along with the anniversary of the 'Arab Spring' by hosting a poster contest, widely publicised via social media, on the topic 'Did you sense the spirit of Gandhi in Tahrir Square'? It drew the theme and the entries not only from Egypt and India but also from several other African countries and succeeded in integrating the most recognisable Indian icon with the most important political event in the region. The contest was India's way of saluting the Gandhian spirit of the 'Tahrir Square' revolutionaries.

This is a clear example of a successful 'soft power' projection through public diplomacy. Soft power has been viewed as a crucial instrument with which India could wield influence as a global actor.[7] It is seen as providing India with an edge over China, as the preferred, softer Asian alternative with a rich, diverse, democratic culture that seems to fit in much better with established norms in the Western-influenced world order.[8] Indeed, as Joseph Nye points out, the limited success of Chinese (and Russian) soft power initiatives can be attributed to the fact that their soft power is projected only through government, while civil society voices are stifled, a factor that gives democratic India an inherent advantage to work with.[9]

Over the past decade, India has invested significant resources in public diplomacy using traditional and new approaches to build and leverage its soft power. This new public diplomacy tool is a function of changed beliefs of the foreign policy-making elite about the uses of new social media networks in engaging with non-state actors around the globe. This also projects that India's new public diplomacy seems to have met with some success—albeit patchy—in augmenting its soft power. The traditional work of diplomacy has seen a

greater role of public diplomacy because of the new communications technology. In addition to the State-to-State diplomacy, there has been a shift from State-to-people, people-to-State, and people-to-people type of exchanges. This form of public diplomacy is transnational and it is now possible for a large number of people to participate in sustained and decentralised communication with governments.

The nature of digital media is a break from traditional forms of print and broadcast communications. These are one-to-many communication technologies. The internet is essentially a many-to-many type of information technology. The internet enables more and different actors to get involved in political and diplomatic processes in a transparent and perhaps accountable manner, leading to 'democratisation of diplomacy'. It multiplies and amplifies the number of voices and interests involved in international policy-making, complicating international decision-making and reducing the exclusive control of States in the process.

The new form of decentralised statecraft reflects a 'triple paradigm shift' cumulating on a common infrastructure for the first time in history. The three primary information networks of I.R. are—trade, personal communications and mass media. The infrastructure that conveys goods around the globe has shifted over the centuries from ships to rail to highways. Our communication networks have changed from post to telegraph to telephone to the internet. Our mass media has moved from print to radio to television to 'facebook'. Today, all three of these systems operate largely on the internet.

The Department of Public Diplomacy in the Indian Ministry of External Affairs, used 'Twitter' during the evacuation of Indian nationals from Libya in 2011, and it was a real eye-opener. The Department used it to put forth timely information about the evacuation schedule and received invaluable information from the ground about the requirements of Indian nationals in distant parts of Libya. They got large dollops of appreciation from tweeple (Twitter users) who appreciated the effort that the Department of Public Policy was making in using new media. It also turned out to be a pleasant surprise that a Government of India venture could be so refreshingly unconventional or non-sarkari.

As the pace of economic globalisation intensifies, the role and importance of NGOs is being realised, while the welfare role of the State diminishes. These groups utilise IT tools such as the internet and e-mail to source and

disseminate information on a wide variety of developmental issues, from environmental protection to democratic inclusion of minorities in domestic political processes. The fact is that technologies such as e-newsgroups, e-mail, databases and websites provide the electronic means, whereby ideas and discussions on various issues can be advanced and exchanged in real-time. This has led to the emergence of specialist organisations which are more knowledgeable than the State on specific issues. These have become major players capable of influencing policy outcomes at international meetings. Their aggressive, outspoken positions on issues now make them a formidable negotiating force in international negotiations. Increasingly, NGOs are being called upon to lend their expertise to evolving solutions to a variety of problems.

NGOs have been swift to adapt to the potential of the internet to increase their influence in international affairs. Communication and advocacy is their core business and they devote significant resources to making the best use of the internet. Amnesty, Oxfam, Greenpeace, Human Rights Watch, all have had a powerful web presence for years and are regularly used as a primary source of information by the web-surfing public. But the internet has facilitated an even wider diversification of actors by enabling groups without a collective voice hitherto to find one.

Interestingly, I.R. can no longer be construed solely on the interaction amongst nation-states. In the evolving international landscape, the State is but one actor setting the diplomatic agenda. Powerful multinational players are utilising information and communications technologies to sensitise global public opinion on a host of issues previously considered 'domestic'. For example, by adapting production processes to a digital international trading system, global corporations can easily relocate operations. This has had the effect of adding a new dimension to the diplomatic agenda and of diluting the governments' role as regulator of fiscal and monetary policies, transforming them into negotiators. Capital and financial markets have become internationally structured such that instability in one country can trigger negative responses in several States.

Global firms are more powerful than many governments, often placing the latter in the position of negotiators instead of regulators of the domestic economy. As economic processes become increasingly global in orientation, domestic fiscal and monetary policies become less effective. Diplomacy is shifting from State-centred interchanges to transnational interactions in which global firms, NGOs and the global media have become key actors in the

diplomatic arena, influencing foreign and domestic policies, somewhat eroding the State's authority and sovereignty in the process. The 'internationalisation' of economic, social and security issues beyond the capabilities of the nation-state are creating new diplomatic channels in which, States through bloc associations and supra-national governance, are attempting to deal with these issues.

Digital Technology in Government-to-Government Diplomacy

The core of diplomacy is communication. When communication methods change, as is happening in the present context, diplomacy must adjust. In 2007, Maldives became the first country to unveil the world's first virtual embassy. The Maldives virtual embassy was soon followed by embassies representing Sweden and the Philippines. This virtual embassy was designed to allow new avenues for diplomatic representation and negotiation, especially for small and developing countries that have limited diplomatic outreach in the 'real' world. It was the brainchild of Diplo Foundation, a non-profit organisation which works to assist developing countries participate meaningfully in international affairs.[10]

Speaking ahead of the opening ceremony, the Maldivian Minister of State for Foreign Affairs Abdulla Shahid emphasised how information technology and particularly the internet can be harnessed by small countries to enable them to participate meaningfully in international relations. He explained that Maldives is a small country but a well-known tourist destination that has experienced rapid economic, social and political development over recent years by use of IT to best advantage.

Information-Communication-Technology (ICT) enables governments to promote diplomatic services by quick and efficient communication and enables them to share databases, resources and skills. Inter-government diplomacy is transactional and interactional in the relationship between government and its agencies and other foreign (nations) countries. In such a web of relations, government interacts and depends on other governments/States to effectively deliver services and allocate responsibilities. The role of ICT in government-to-government diplomacy encompasses three critical dimensions: internal, external and relational as noted by Hirst and Norton (1998).[11]

Internal transformation refers to the use of ICT to improve the efficiency and effectiveness of internal functions and processes of the government by inter-relating different departments and agencies. Thus, information can flow

much faster and more easily among different governmental departments, reducing processing time, paperwork bottlenecks and eliminating long, bureaucratic and inefficient approval procedures. It equally facilitates storing and collecting data, reduction of labour costs and information handling costs and the speed and accuracy of information processing.

Externally, ICT opens up new possibilities for government to be more transparent to citizens and business, giving access to a larger range of information collected and generated by the government. Relationally, ICT adoption may enable fundamental changes in the relationships between the citizens and the State and between nation-states with implications for the democratic process. Horizontal integration of services can be realised more effectively, enabling the integration of information and services from various government agencies, to help citizens and other stakeholders to become seamless.

Digital technology enables transmission and use of all of these protected materials in digital form over interactive networks. The process of 'digitisation' allows the conversion of such materials into binary form, which can be transmitted across the internet and then re-distributed, copied and stored in perfect digital form. While the transmission of text, sound, images and computer programmes over the internet is already commonplace, this is also true for transmission of audio-visual works such as feature films, as the technical constraints of narrow bandwidth begin to disappear. Materials protected by copyright/related rights, spanning a range of information and entertainment products, constitute much of the subject matter of e-commerce.

Intellectual property rights provide the foundation upon which innovation is shared, creativity encouraged and consumer trust reinforced. But the digital world poses a new challenge—how to manage the balance when the consumer is the creator, when the marginal cost of copying is zero, when enforcement of existing law is extremely difficult, and when 'free' access to information and content is considered by many to be a right. These are new challenges of the future which may demand radically new approaches to management of information and intellectual property.

The rapid growth in the volume of patent applications is creating patent 'thickets'. These occur where inter-related and overlapping patents result in lack of clarity about who owns the patent and as a consequence, where to go for the licence. The technology sector has become increasingly litigious, which becomes a problem when it stifles innovation or acts as a barrier to new market

entrants. Since the norms for protecting intellectual property are not very clear, it requires a relook at the international laws governing technology exchange. However, diplomats need to have more clarity in order to negotiate intellectual property interests for the nation. There is thus a requirement to formulate new laws and regulations to overcome this ambiguity at the national and international level.

Today, there can hardly be any secrets on the internet. Anything sent over the internet, even encrypted, can be potentially compromised. The World Wars saw messengers captured, bridges blown up, telephones tapped, goods hijacked; but spies or whistle-blowers always found ways to tap information securely held. But the internet brings a new dimension to the security of information with implications for I.R. Private information when made public, may have a swifter and more profound impact on the conduct of world affairs. Hackers have demonstrated how easily useful material can be found even when an organisation does not want it to be seen; and recent scandals over the loss of personal data from British Government systems show how easily information can be lost.

The steady trickle of leaks about the British Government's policy and legal opinion on the war in Iraq led to damaging the reputation of the then prime minister. All such material is often freely available world-wide on the web. Another striking example is of how appalling images of the US' treatment of 9/11 suspects received instant and global circulation through the internet. The effect caused permanent damage to the reputation of the US, weakening its moral authority in the world and fuelling jihadist attacks in different parts of the world. It also garnered a lot of negative publicity for then President George W. Bush. This would probably have happened without the internet, but the internet amplified and extended the impact. Similarly, diplomatic rivals, including both State and non-state actors (such as terrorist organisations), may try to hack into government systems and extract information of use to themselves or even tap into social networks of the country to get a sense of public opinion.

Yet another implication is that the internet itself becomes a vulnerable part of every nation's critical infrastructure, where virus or worm attacks can be easily generated. In the past few years, very often such virus attacks have brought large parts of the internet and many of the systems connected to it to a grinding halt. In May 2007, a cyber attack launched against Estonia severely damaged business in the country and prevented it from communicating or making its case public for days. The sophistication and

scale of the attack and its precise targeting strongly suggested a State-sponsored action.

The infrastructure of the internet has in practice proved to be remarkably resilient. Security solutions have been keeping just about one step ahead of the hackers, fraudsters and cyber-saboteurs. This is achieved mainly through constant vigilance, innovation and investment of the major IT companies—Microsoft, Cisco, Google, Yahoo and others—often working in close cooperation with governments. Nevertheless, future threat to the internet's integrity is likely to come as much from constraints on capacity with ever more and larger files travelling across it, as from hostile attacks. 'Cloud computing' today appears to provide one solution, but it may have some of its own perils, yet to be discovered.

Governance of the internet has also been a subject of international discussions. The current US-dominated structure has served it well, but this may not be adequate to meet the challenges of the future. The European Union (EU) has recently challenged US hegemony in global internet governance. Just as it took many decades to agree on an international 'Law of the Sea', it may take an equally long time to agree to anything beyond the existing, relatively informal (and benign) structures for the internet. In the meantime, supply and demand will continue to grow exponentially, and there will always remain a virtual as well as physical ungoverned space, from which internet traffic and content can spread ubiquitously.

In summary, global interdependency has spawned new security concerns transcending borders which domestic policies cannot adequately address. Traditional areas of State responsibility such as defence, economic management and even foreign policy are now being co-ordinated at the supra-national level, e.g. the EU, or regional level, like the Association of Southeast Asian Nations (ASEAN).

ICT has been instrumental in opening up new avenues for cooperative security among a set of nations. ICT acts as common infrastructure for the integration of 28 member-states of the EU enabling the seamless flow of intra-EU economic, political and defence processes. With a common currency, the Euro, digital economy has assumed an enhanced role in the cumulative economy of Europe.

Presently, the internet is under the overall control of the US government. There is much debate about the future of internet and about who governs it. India is not comfortable with the proposal of ICANN (Internet Corporation

for Assigned Names and Numbers) about bringing all stakeholders into internet governance which would dilute the role of the national government. There is not only need for proper international legislative authority at the international level, but also clarity and convergence between the Ministry of External Affairs and the Ministry of Communications and Information Technology in India. Information security in the cyber space is emerging as the most vulnerable area that may spark future conflict.

Challenges for India

India like many other countries is also on the learning curve, on how best to leverage digital technology for protecting sovereign priorities in cyber space, while being globally participative—as expected of a democratic country. On the other hand, being an open democratic nation with vast possibilities, the vulnerability that India may face in the globalising and digital world may be quite unique.

As the information era unfolds, new actors are utilising IT and communications technologies to engage States in a new type of diplomacy, one driven by technology. Developed nations have been quick to adapt to these technologies and recognise that in the emerging diplomatic environment new electronic mechanisms must complement traditional diplomacy. Developing countries such as India have indeed embraced the idea; but a more concerted effort is required by Indian diplomats to leverage IT without being restricted by social media platforms.

Diplomats eventually need to become masters of the internet, not just to know where they can best collect the most reliable information to meet deadlines for decision-making, but also to know how to exert maximum influence on public debate through this medium. Face-to-face negotiation will always remain their prerogative, but the context in which they undertake it and the forces at work in those negotiations are changing rapidly. The internet is at the heart of those changes—already beginning to be recognised as the 'Internet of Everything'.

NOTES

1. Amitav Mallik, *Indian Science & Technology: A Status Review*, Pragun Publications, in association with Observer Research Foundation (ORF), Delhi, 2006.
2. India conducted its first nuclear detonation, described as a 'peaceful nuclear explosion (PNE)' code-named 'Smiling Buddha' on May 18, 1974. See www.fas.org/nuke/guide/india/nuke/first-pix.htm. (Accessed June13, 2014).
3. Government of India took a bold step in the year 1988 to create a new office of Adviser,

Defence Technology at the Embassy of India in Washington DC to negotiate and reverse technology denial decisions by the US against India. The author had the honour of creating this new office and negotiating with the Pentagon, the US Department of State and the US Department of Commerce for successfully reversing many technology denial cases against India. The seeds for Indo-US high-tech cooperation sown during the extended six-year tenure of the author bore many immediate fruitful results and paved the way for subsequent Indo-US technology cooperation under NSSP (Next Steps in Strategic Partnership).

4. "START - Russia and U.S. Sign New Strategic Arms Reduction Treaty" *, The New York Times,* April 8, 2010, at www.nytimes.com/2010/04/09/world/europe/09prexy.html. (Accessed June 13, 2014).
5. See no. 3.
6. "The-science-technology-and-innovation-policy-government-of India 2003", at http://dst.gov.in/sti-policy-eng.pdf (Accessed June 13, 2014).
7. Shashi Tharoor, 'Indian Strategic Power: Soft', *Huffington Post*, June 26, 2009, at http://www.huffingtonpost.com/shashi-tharoor/indian-strategic-power/so_b_207785.html (Accessed June 13, 2014).
8. William Callahan, "Themes in the India–China debate over the future world order", at www.acedemia.edu/.../Digital_Public_Diplomacy_and_a_strategic_narrative_for-india (Accessed June 13, 2014).
9. Joseph S. Nye, "What China and Russia Don't Get About Soft Power", *Foreign Policy*, April 29, 2013 at http://foreignpolicy.com/2013/04/29/what-china-and-russia-dont-get-about-soft-power/ (Accessed June 13, 2014).
10. Diplo Foundation, "Maldives Unveils World's First Virtual Embassy", at http://archive1.diplomacy.edu/poolbin.asp?idpool=463 (Accessed June 13, 2014).
11. Peter Hirst and Michael Norton, "Electronic Government: Information Technologies and the Citizen", UK Parliamentary Briefing Papers, POST PN 110, Parliamentary Office of of Science and Technology, February 1998, at http://www.parliament.uk/post/egov.htm (Accessed June 13, 2014).

PART II

Technologies of High Impact on International Affairs

3

Defence Technologies: Game Changers for International Affairs

Introduction: Game Changing Defence Technologies

The 20th century was witness to a sea of changes in defence technology that for the first time expanded to the fourth dimension of outer space and now in the 21st century, it is expanding to the fifth dimension of cyber space. The superpower rivalry and the race for technological superiority fuelled intense research and development (R&D) and rapid growth in defence technology, ably aided by scientific inventions and technology innovations. While guns and tanks became more powerful with extended range and accuracy, the real game changers were advances in electronics, sensors, rocket propulsion, missile guidance and control systems and advanced materials. Advances in computers and integration of sensors with Information-Communication-Technology (ICT) pushed the envelope of defence capabilities to new paradigms, while miniaturisation in electronics and mechanical engineering transformed the size and weight of military systems.

The concepts of strategic defence and diplomacy have undergone significant transformation, driven mainly due to technology advances and the limitless capacity of the human brain for innovation. Artificial Intelligence (AI) and robotic autonomous systems can potentially add revolutionary capabilities for defence and security. A brief review of this phenomenal evolution in military technologies is presented here, to highlight how the arrival of digital electronics and satellite networks has contributed to the recent

Revolution in Military Affairs (RMA) of network-centric strategies and operations that are proving to be game-changers in global politics and balance in international affairs.

The nuclear weapon (NW) and its long-range delivery was a major game changer when it arrived in 1945 on the international scene. Nuclear-missile deterrence continues to be one of the most important instruments of diplomacy in international relations (I.R.) in the context of balance of power and international stability. Of the Weapons of Mass Destruction (WMD), international diplomacy has successfully achieved consensus on a global ban on the use of chemical and biological weapons, but NW continue to be relevant, more in some regions of the world than others.

However, WMD threats are now perceived more from rogue States or non-state entities, albeit with covert support from some State actors seeking asymmetric advantages. Deterrence dynamics for this type of threat will perhaps demand new approaches based on advanced technologies for high situational awareness and high precision delivery weapons to pre-empt the attacks and nullify the threats. Layered defence against multiple simultaneous missile attacks, with high accuracy hyper velocity missiles, or energy beam weapons is gaining major importance for the future. Technology is thus providing newer alternatives for deterrence and war prevention.

Negotiations with rogue States/non-state entities will pose a new range of diplomatic challenges in this age of instant worldwide communication and 24x7 worldwide TV that brings about new sensitivity. The future will demand efficient intelligence analyses, quick decisions and prompt actions for managing sensitive situations. Diplomats in the future will need to act fast and with more prudence.

In the new paradigm of coercive diplomacy, Comprehensive National Power (CNP) would finally allow powerful nations to compel others to comply with their own foreign policy priorities. Conventional defence, involving pre-emptive counter-force, is also gaining regional significance and here again, the science and technology (S&T) strength of a nation becomes critical to provide actionable intelligence for precision strike capability with high-tech weapons. Technology is moving to electronically de-capacitate the enemy military command and control infrastructure for initial gains, and decisive techno-military power is replacing the might of traditionally large armies that depended on the number of boots on the ground. The world-over, armies are getting leaner and meaner with modern technology.

Future wars are likely to be less about territorial disputes and more about issues of regional or global influence on basic resources such as energy, water and environment. Economic divide or religious fundamentalism will continue to be major causes of conflict. Hence, the power-dynamics of this new world would be very different and increasingly dependent on techno-economic as well as techno-military superiority. This chapter will present an overview of this game-changing dynamics where S&T will play an even more important role in the future of defence and security of nations.

As the danger potential of technologies increases, there is growing international focus on a world without devastating weapons and on preventing possible misuse of high-impact technologies. However, as long as major powers continue to depend on nuclear-missile capabilities as insurance against WMD threats, real nuclear disarmament will remain a challenge for international diplomacy. Fortunately, S&T advances are providing non-nuclear techno-military deterrence and opportunities for increasing the role of S&T in the security calculus. These include advanced force-multiplier technologies for missile defence, network-centric capability, aerospace dominance, underwater technologies, advanced miniaturised sensors and robotic capabilities. A new class of energy weapons may probably change the future complexion of defence technologies.

Advanced technologies of Command, Control, Communications and Intelligence (C^3I) and precision strike capabilities of remotely operated combat Unmanned Aerial Vehicles (UAVs) today, provide new means for pre-emption and coercion. While such drone-diplomacy is being tested for the first time by the US against a rogue non-state entity, the demonstrated stand-off capability provided through technological sophistication is gathering an important deterrence element without the use of WMD. Given that non-state entities or groups cannot have significant fighting capability without covert support from some State entity, the diplomatic challenge of the future will be about dissuading rogue States from using terrorist organisations to serve their limited foreign policy objectives or regional aspirations through rogue means.

Unfortunately, technology diffusion has been instrumental in enhancing capabilities of smaller fundamentalist groups against larger forces of nation-states. Will the new world need new approaches to technology control to contain sensitive technology proliferating into wrong hands and rogue minds? As new high-impact technologies such as space capabilities and cyber weapon technologies assume increasing deterrence values, the international community

of foreign policy experts and diplomats will be faced with a new range of challenges, of how best to reduce the relevance of WMD and other dangerous technologies, and of how best to balance regional priorities for maintenance of global peace.

As reliability of missile defence, using both kinetic as well as energy beam weapons improves, the impact of nuclear-missile deterrence will certainly reduce. However, technological sophistication will continue to rise, thus offering outer space or cyber space based techniques to provide other crippling deterrence options. Protecting sensitive technologies with denial-based foreign policy priorities would again gain momentum. In the ultimate analysis, future sensitive technology exchanges among nations or multinational companies will be based on 'Responsible Ownership' of technology.[1] It is in this context that future threats emanating largely from irresponsible non-state actors and rogue States that support them will need to be diffused.

The future may see some interesting revolutionary changes in technologies of high importance to defence and security that would not only impact military affairs but also economic affairs. Technologies related to energy and environment could determine global peace and stability. As the line between defence and civilian technology becomes thinner, traditional defence technologies will combine with new enabling technologies and several hitherto fictional capabilities may become real-world capabilities. In the digital world of today, as technology for instant access to global information combines with network-of-network based decision-making one can anticipate major transformation in international affairs where global balance of power and peace will depend on control of human intentions and technology choices. Defence technology is a vast subject on which hundreds of books have been published. This chapter will attempt to highlight only those aspects of defence technology that will have a large impact on international affairs.

Evolution of Defence Technologies and Impact on International Affairs

It is interesting to examine the reasons as to why there has been no use of NW since the first and only use in 1945. One of the foremost is the impact of modern defence technology that has evolved to offer several options with non-nuclear strike that can be more effective than NW. Another reason is that NW with their unacceptably large loss of human life and the devastating after-effects of exposure to radioactivity by the survivors has almost made

them unusable. Defence technology advances of the past several decades have been so phenomenal that any major war today has become unaffordable to most progressive nations. Unlike in 1945, NW capability is now available to more than nine nations and hence a NW strike against any nation with NW or its ally is bound to invite a retaliatory NW attack, which would perhaps be more punishing than the first strike; such a cost intensive option for war where both parties suffer unacceptable damage and destruction has become a No-Win situation. Some credit for this must go to technologies that have not only enhanced conventional military capabilities but have also made conventional war-mongering more transparent, much more expensive and hence, a low probability in the future.

The other aspect that makes war a very hard choice is the globalising nature of our world today, where interdependence and interconnectivity will ensure that all will have to suffer to some extent if a major war indeed breaks out. Hence, while the value of peace has gone up many-fold at the same time, the cost of war has also increased many times, due to the integration of economics and development through scientific research and technological innovation. Technology has enabled human society to aspire for wealth creation and stability that can be upset by any war situation. The real power is shifting to techno-economic superiority, where conventional military engagement can have only limited utility.

New defence technology options made possible by technological sophistication are changing the very doctrines of warfare from surprise attack by a large army (World War I) to a massive devastating strike by WMD (World War II) to a high-tech war of today that is fought more in the electro-magnetic spectrum than on the ground. In the middle of the 20th century, World War II saw extensive use of tanks, airplanes and battleships and the introduction of radar, sonar and advanced avionics. Soon to follow were the ECM and ECCM (Electronic Countermeasures and Electronic Counter-Countermeasures) ushering in the elements of Electronic Warfare (EW). The range and accuracy of guided missiles kept increasing steadily, thus introducing high precision weapon delivery using advanced tracking with microwave, lasers or Global Positioning System (GPS) guidance technology.

Computers took over complex tasks to help machines and weapons become smarter. Digital electronics transformed sensors and the Command, Control, Communication, Intelligence, Surveillance and Reconnaissance (C^3ISR) networks offer improved intelligence. Military satellites orbiting the earth provided a quantum leap in networked capability for sharper and instant

situational awareness, transforming the battlefield like nothing before. Information became the principle instrument of power and globalisation is making the world appear smaller with increasing interdependence.

All this was driven by scientific discoveries and technological innovations at every level and in diverse fields of interest to benefit national security and comprehensive national power. Economy and knowledge became the main enablers for most human aspirations. The high cost of war started becoming totally wasteful and unaffordable, as technology brought about enhanced transparency and new alternatives to conflict resolution. Even the politics of technology controls has changed from control of entities to management of intentions. Conduct of statecraft and diplomacy has thus changed quite dramatically in the short span of the last three to four decades, thanks mainly to the impact of technology on global affairs and international relations. This changing paradigm however, does not mean that conventional military force is about to become obsolete, but it certainly will have to get leaner and smarter.

Defence Technology Environment

Advanced defence technologies have always provided the superiority needed by States for defence and security as well as for power positioning in international affairs. Advanced countries that possess such defence technologies have always been protective about these and developing countries that lagged behind in technology have always aspired for such technologies. The technological revolution of the past few decades has however, created a significant shift in the security perceptions of individual nations.

India's rapid techno-economic progress as well as the nuclear test of 1998, helped create a paradigm shift in the global perception of India as a potential emerging global power. This along with the market forces of globalisation has changed the basic precepts of defence, offence and security for India. The defence technology architecture for India in future is therefore, likely to be very different from the traditional approach to military modernisation of the past. It is important to understand this change from an external policy perspective, so that defence and foreign policies could combine together, to better achieve the national objectives of future technology acquisition and power positioning for India.

An interesting change in the 21st century is that most critical technologies for defence are of dual-use nature and the rapid advances in civilian technologies are often feeding military-strategic requirements. Since these

technologies are also critical to economic competitiveness and industrial development, global corporate sectors that develop and control such technologies are becoming the major players in international technology exchange, while the role of government agencies is becoming more of a facilitator than a controller. Of course, when it comes to the question of national security, all national interests automatically converge, and the corporate sector behaves very responsibly, to stay within government guidelines for international interactions.

Enabling technologies such as information technology, data fusion, artificial intelligence (AI), robotics, nanotechnology, biotechnology etc. are transforming the spectrum of technology capabilities. Advances in sensors, precision guidance, satellite systems, autonomous systems, energy beam weapons etc. are offering a range of new capabilities for offence and defence. While these do represent the universal wish list of any modern defence force, the actual architecture of defence technology for a specific country is governed by several factors such as the threat perceptions, indigenous techno-industrial base, economic strength, and of course, the country's defence strategy and security doctrine.

For India, the experience of the 1962 war with China brought about a major change in defence policy, by which defence R&D and defence production got the much needed push in the overall national defence planning process. Starting with modest efforts at import substitution and product upgrades, indigenous defence technology in the country gained real momentum, only after restrictive technology embargoes were imposed on India by the West as a reaction to the 1974 Peaceful Nuclear Explosion (PNE).[2] Interestingly, for India, this helped to fuel the urgency for achieving a high degree of self-reliance in technologies critical for defence and development. However, the priorities of societal development have always competed with defence allocations in India, and as a result, India's defence budgets were very modest till the 1990s. Defence modernisation typically got only about 10-15 percent of the total defence budget and defence R&D got a very small share of less than 2-3 percent of the defence budget. Teething problems, faltering progress, heavy dependence on imported Soviet equipment, as well as the struggle to compete with other modernising forces of the world—all this is history of India that is well documented and well known.

The introduction of computers and digital electronics received a major boost in India under the leadership of India's youngest Prime Minister, Rajiv Gandhi, after the 1984 elections. The opening up of the Indian economy in

1991 was a major milestone that saw foreign direct investment flow into the country. The Y2K push for software expertise at the turn of the century, saw an impressive performance by Indian engineers and software professionals, and India started emerging as a powerful international player in ICT as well as in business process outsourcing (BPO).

In 1988, the Indian Government established the new office of Adviser, Defence Technology at the Embassy of India in Washington DC, as a major techno-diplomacy initiative to find ways of softening the US technology controls for India's high-tech requirement in major R&D projects such as the Light Combat Aircraft (LCA).[3] This initiative paid rich dividends for Indo-US cooperation in several defence technology areas, where the US defence industry pushed aggressively for Indian market access. This therefore, proved to be a kind of win-win solution, where India also gained access to sensitive technology, with case by case negotiation with the US State Department and the Pentagon.

However, by mid-1990, India was again on the back-foot during the Comprehensive Test Ban Treaty (CTBT) negotiations at the Conference on Disarmament (CD) just around the time of the indefinite extension of the Nuclear Non-Proliferation Treaty (NPT). India by then had developed indigenous nuclear technology capability despite being targeted by technology denials of the Western alliance. However, India maintained exemplary commitment to non-proliferation with demonstrated responsible ownership of nuclear technology. India stayed out of the NPT because of its discriminatory nature and also refused to sign the CTBT as it compromised its national security interests. In fact, India's mature and well-informed negotiations on CTBT at the CD by the then Indian Ambassador (Ms.) Arundhati Ghose created history demonstrating how a single developing nation could be resolute on an issue of supreme national security interest.[4]

By 1995, India was already surrounded by NW-capable China that helped Pakistan acquire NW for itself, to counter India's conventional military superiority. Given the grave nuclear threat from known adversaries on either side with a history of war, it was imperative for India to end the long nuclear ambivalence and declare itself a NW power. This was achieved in May 1998 with a series of nuclear tests—Pokhran-II—to establish its nuclear credentials.[5] Pakistan was quick to follow with its own tests, going nuclear, overtly confirming Indian claims that Pakistan was just a step from having a NW. Subsequent findings also confirmed that China, despite being a core NPT member, provided all guidance and assistance to Pakistan to go nuclear.

Concomitantly, Pakistan's irresponsible and clandestine nuclear trade under A.Q. Khan also got exposed and international equations in the South Asian region changed significantly and permanently.

Armed with the assurance of nuclear deterrence the Pakistan Army was quick to attempt a deceptive takeover of critical areas of the Kargil heights while Pakistan's civilian leadership appeared to pursue peace initiatives with India. Such blatant deception was unheard of in modern I.R.; consequently, India took swift military action to diffuse the situation quickly, in what is now known as the Kargil War. This prompted a major review of Indian defence preparedness and a comprehensive report was published on 'Higher Management of Defence' for India (better known as the Kargil Committee Report).[6] But despite the rude awakening of the Kargil War, the pace of defence acquisition, modernisation as well as R&D, has been very sluggish in India. This is due to many reasons including political hesitation, poor long-term military planning, poor record of the government in policy implementation and serious weaknesses in decision-making even in matters of national security.

Paradoxically, while defence technology development and defence acquisition for modernisation have been slow in the country, rapid strides in information technology by Indians in India and abroad, and an impressive rate of economic growth since the turn of the century, has changed the international environment for India. Thanks to the 9/11 incident, US priorities changed suddenly, to high focus on homeland security, and the sanctions on India-Pakistan for violating NPT were lifted by the US in the interest of its War on Terror. Indo-US strategic and technology cooperation under the well known NSSP got revived by 2004 and the path-breaking US-India nuclear energy technology agreement was initiated in 2005 and concluded swiftly by 2008.[7]

Most political observers saw this as a start of some kind of strategic partnership between US and India, presumably to create a counterweight in Asia against China's rapid military advances and expansionist plans. Interestingly, US was able to persuade the Nuclear Suppliers Group (NSG) to accept India as a legitimate and responsible partner for civil nuclear trade, which could bring good business to US and help in creating thousands of high-tech jobs in the US. Given the fact that the NSG was formed specifically to target India for its 1974 nuclear experiment, the complete turn-around in just about 30 years, shows how fast political priorities can change in the dynamics of I.R. These developments saw unique coordination between the Ministry of External Affairs and the Ministry of Defence that enabled Indian

defence scientists to join hands with Indian diplomats negotiating issues with the US and the international strategic community. This was a stellar performance of diplomacy in technology affairs!

For a progressive country like India with a very hostile neighbourhood and a history of border wars, conventional military capabilities for eventual border conflicts will continue to be important for the foreseeable future. In addition, armed forces will have to be ready to deal with internal security challenges including insurgency and terrorism. Proxy war/sub-conventional war is a major challenge for India and specific technologies for fighting such low-intensity conflicts will need major attention in the future. These may include sophisticated intelligence surveillance apparatus, secure communication infrastructure, effective use of ICT for timely warnings of threats and quick decision-making for rapid response. Much like conventional war-fighting, enhanced situational awareness and well-coordinated response to threats, including preventive actions will be crucial in this Low Intensity Warfare. New technologies for detection and diffusion of Improvised Explosive Devices (IEDs) will have to get priority funding support and new focus will be needed for innovative application of existing technologies or combination of capabilities.

Leveraging ICT for prevention and management of threats to human security inside the country must thus form the main thrust of what is now commonly known as homeland security. It is in this context, that a review of defence technology architecture for India becomes important, to address both external threats and also international security.

India's defence and security planning will require better foresight, which alone can help India acquire defence and security technology capabilities, that are critical not only to India's long-term national security, but also to India emerging as a major world power. As in most security affairs, techniques and technologies for situational awareness and rapid response are becoming as critical as strategic capabilities. Technologies for basic battlefield capabilities 'to Sense, to Reach, to Deny and to Destroy' will need to be maintained at the cutting edge of readiness, while strategic technology capabilities will have to match the best in the world.

With its unique set of real security threats across all its land borders, India has an unenviable task of managing the imperatives of defence and development in the new age of fierce techno-economic competition. Conventional military superiority in terms of quality and quantity of modern

war-fighting equipment will certainly remain relevant for preventing unpredictable adventurism by troubled neighbours like Pakistan. But in the event of a limited war breaking out, India will also need modern information based war-winning technologies, as well as cutting-edge futuristic capabilities. Hence, besides the usual platform upgrades, military modernisation in India for the immediate future will have to concentrate on the enhanced use of versatile technologies for situational awareness and early intelligence for possible preventive action. Technology and diplomacy must combine effectively for this challenge.

For a limited border war scenario, India will have to acquire robust early warning and surveillance capabilities and integrate the C^4ISR apparatus effectively for network-centric strategies. This should vastly improve the 'sensor-to-shooter time', which is very important in today's transparent battlefield. Other key strengths must include effective use of UAVs for surveillance as well as combat, multi-spectral sensors and data fusion, better signal processing technology, improved radars, military satellite systems, missile defence technology, enhanced underwater technology etc. While the navy may have to trade priorities between littoral warfare and blue water capabilities, the air force will need to establish clear dominance in its sphere of influence with 24x7 precision-strike capability.

There is an urgent need to mobilise space assets for better surveillance and coordination of integrated military operations. Missiles and missile defence technology will have to keep pace with developments in the world, as smaller adversaries can pose serious threats when assisted by more powerful partners. Indigenous capabilities will be crucial in critical technology areas such as advanced materials, smart sensors, electronic and cyber warfare, missile defence, directed energy weapons (DEWs) and counter-space technologies. Foreign dependence on all such critical technologies must be minimised, to reduce the vulnerability to possible future technology controls by advanced nation groups, particularly during conflict situations. A high degree of energy independence will also be critical for India in future, as tensions regarding energy shortages will become more acute.

National Security and Defence Modernisation Priorities for India

The techno-military profile of India in the future has to match the country's overall image of a world class power by 2025. India must therefore emulate the best in the world in terms of techno-military transformation, but temper it with due regard to its economic capacity to bring-in rapid transformation.

Looking at the world trends in defence technology and identifying what suits the Indian requirements best, will thus be key to relevant and effective techno-military transformation for India. Although a network centric RMA on the scale of the US may be too expensive for India, it is nonetheless important to factor-in some major elements of the RMA that are taking shape in the advanced sections of the world, where India must make a mark as a future major power.

Taking a look at the world's sole techno-military superpower, one can realise that the most important element of the recent RMA has been the integration of ICT with war-winning doctrines. While the basic military systems of the present time may look similar to their predecessors—tanks, aircraft, naval platforms, missiles, military satellites etc. it is the technologies of sensors, surveillance, targeting, precision guidance that make such 'legacy' systems much more potent. These now need to be strengthened further with 'informationalisation'—a word coined by the Chinese.

The pace and penetration of ICT has enabled unprecedented levels of connectivity, coordination and situational awareness, making network-centric operations possible on the actual battle-front in real time. From information gathering sensors on/near the battlefield to satellite-based systems in outer space, the volume of useful military-usable information can be massive—leading to a race for 'information superiority' for quick decision support and strategic planning. 'Decision superiority' which entails efficient processing of intelligence information for decision support, will be crucial for the future and technologies that combine to provide such an advantage will be vital in future.

The rise of insurgency and militancy largely due to weak governance and simultaneous rise in cross-border terrorism by adversarial neighbouring countries has compelled India to pay greater attention to internal security, perhaps at the cost of external military capability. India's inability to develop an effective strategy for hard power projection as well soft power leverage, has historically limited the country's foreign policy options in dealing with its neighbours. As a result, India's strategic influence in its own neighbourhood has remained limited. India's adversaries are bolder in making India bleed through a 'thousand-cuts' strategy because India has failed to create the image of a decisive powerful nation that will not tolerate such nonsense.

In future, the techno-military capability of India will have to match not only its immediate national security perceptions but will also have to create

future capabilities for power projections commensurate with its economic rise to a great power status. The defence technology architecture for the country therefore, will have to be crafted with great foresight and careful planning. Given the thin line between defence and civilian technologies, and the realities of the market forces of globalisation and interdependence, an integrated approach to defence technology planning will be essential to developing requisite capabilities for future.

Of late, India has made some concerted modernisation efforts such as upgrading its Intelligence, Surveillance and Reconnaissance (ISR) network, smart bombs for precision strike, missile defence capabilities and triad based nuclear deterrence, as it competes with the nexus of China and Pakistan for regional power balance. The Indian Navy's modernisation plan includes the Aircraft Carrier *INS Vikrant* launched in August 2013, and expected to undergo sea trials, and the carrier, *Admiral Gorshkov* purchased from Russia, being overhauled with latest electronics, sensors and weapon systems, to be inducted as *INS Vikramaditya*.[8] The recent launching of the indigenous nuclear submarine *Arihant* is an important milestone for India's defence modernisation.[9] The Indian Navy will also have to build or acquire technologies for under-sea mine clearing, and advanced torpedoes for hunting enemy submarines. The vulnerability evident during the 26/11 attack on Mumbai brought focus on the need for supporting counter-terrorism activities in the coastal waters.

Highlights of the Indian Air Force plans for modernisation include immediate acquisition of over 400 fighter aircraft of different types including the SU31-MK1 and the French Rafael Medium Multi-Role Combat Aircraft (MMRCA), besides six squadrons of the LCA. Major upgrades to existing fleets are also in progress with negotiations for Fifth Generation Fighter Aircraft (FGFA) already initiated.[10] India is certainly seeking to bolster its rise as an economic power, by reshaping its armed forces into a modern military, capable of projecting power well beyond its shores, and its defence spending has been increasing steadily in recent years. However, the pace of modernisation must accelerate with the robust involvement of major Indian industries and foreign collaboration where appropriate, in joint venture (J-V) mode, as successfully demonstrated by the BrahMos cruise-missile programme.[11] The BrahMos has been developed as a joint venture between the Defence Research and Development Organisation (DRDO) of India and the Federal State Unitary Enterprise NPO Mashinostroyenia (NPOM) of Russia. The missile is named after two rivers, the Brahmaputra and the Moskova. KELTEC (now known

as BrahMos Aerospace Trivandrum Ltd. or BATL), an Indian State-owned firm was acquired by BrahMos Corporation in 2008. Approximately Rs.15 billion ($250.5 million) will be invested in the facility to make BrahMos components and integrate the missile systems. Out of a total share capital of approximately $300 million for the Joint-Venture, India's financial contribution has been over 50 percent.

Another success story has been the Indian missile programme that has already given a series of tactical missiles, as well as nuclear capable strategic Inter-continental Ballistic Missiles (ICBMs) to the country, and which is now focusing on establishing a layered missile-defence capability.[12] The Indian Space Research Organisation's (ISRO's) recent success with the simultaneous launch of multiple satellites in different orbits has important defence connotations because the technology used is very similar to the capability required for launching ICBMs with Multiple Independent Re-entry Vehicles (MIRVs).[13]

Three clear facets of India's current defence modernisation direction are: 1) technological modernisation, especially for enhanced air and sea power; 2) doctrinal innovation designed to create capabilities for rapid deployment of customised combat force; and 3) organisational innovations for decision-making with a quicker response. Technology trends for the future military force structure must clearly be geared towards—(a) Increased emphasis on advanced sensors and information processing (b) Greater precision in all weapons systems and (c) More use of unmanned vehicles for air, land and sea applications. One will see significant increases in R&D in all three areas with a special focus on catching-up with the best in the world. For the infantry on the ground, lighter backpacks, advanced wireless communication sets, night vision devices, shoulder fired missiles and GPS enabled systems are the technologies that will make the difference.

Future combat system designs will probably move towards lighter platforms, with higher inter-operability for inter-Service use, and with an increasing element of stealth technology. Technologies that can reduce or simplify logistic requirements for rapid response and flexible deployment of forces, will be important in shaping the future defence architecture for conventional superiority. Technology trends do indicate greater dependence on unmanned platforms and robotics for land as well as under-water applications.

Importance of air-superiority has been demonstrated amply in recent wars and hence, acquisition of modern multi-role fighters with advanced stealth

characteristics, advanced avionics and weapon superiority must remain the main focus of the Indian Air Force. However, increasing integration of information networks and advanced sensors should clearly be the thrust of indigenous R&D as these can rarely be purchased. Similarly, electronic warfare (EW) elements also need to be designed and developed indigenously, as an EW edge may be the deciding factor for air-superiority in the future. Cruise missiles and Precision Guided Munitions (PGMs) have already proved their advantages and advances in all-weather PGM technology and advanced cruise missiles should be a high priority for India.

Wide access and affordability of Surface-to-Air Missiles (SAMs) will pose a major threat to fighters in low flying missions. This threat will be serious not only for fighters but also for attack helicopters and cargo planes that are more vulnerable. Helicopters will also need devices for protection from shoulder fired missiles that have proved very effective in the hands of militants. Technologies for extending the range and capabilities of UAVs will witness major R&D momentum and satellite based systems will be vital to qualitative improvements in ISR-based early warning capability for any nation.

Growing dependence on satellite-based systems for surveillance and navigation is unavoidable but this also increases the vulnerability of the system. Even critical civilian functions for most nations are now highly dependent on satellite-based systems and protection of such systems will be crucial to defence. Use of a constellation of several mini-satellites for distributed capability is one option that many advanced countries are working on, to reduce vulnerability. It is therefore not surprising, that most leaders in technology have accelerated the R&D on space defence technologies. India cannot afford to lag behind and must quickly develop its own military satellite infrastructure and satellite defence technology. This is an area where self-reliance will be very critical for India because no one will give such technology for love or money.

Although space technologies today are intrinsically linked to defence capabilities, so far outer space has remained free of weapons, with military use limited to a variety of defence support functions. Besides, integration of advances in ICT, imaging and guidance technologies with satellite based systems, advent of DEWs and missile defence technologies will dominate future R&D efforts world over, as countries get more sensitive about possible weaponisation of outer space. The increasing concerns of possible misuse of space based capabilities by rogue elements are likely to bring-in some international norms and restrictions on these technologies. India must

therefore develop core competence in such critical space defence technologies that will be closely guarded by advanced countries in the future.

Another paradox is that most technologies for missile defence have potential anti-satellite capabilities. Hence, R&D on these technologies has been a priority area for advanced nations and India must remain sensitive to this. Missile defence requirements of individual nations however, may be quite unique, and India needs to identify its own priorities. Major political and strategic decisions regarding specific missile defence priorities and military satellite programmes are needed urgently for strategic clarity and hence, India urgently needs an integrated policy approach for harmonising space and defence plans and projections.[14] India needs policy driven changes for building robust military satellite programmes and a major momentum for well-directed futuristic R&D for adequate self-reliance in these areas.

It can be concluded that while the above discussion is aimed at identifying broad areas of technology priorities for defence and security requirements of the country, the defence technology architecture for India must go beyond just specific requirements. Defence R&D in the country needs to be totally revamped along the Defense Advanced Research Projects Agency (DARPA) model, wherein the thrust of R&D must be in futuristic enabling technologies, such as smart materials, nano-sensors and circuits, bionics devices, advanced computing, robotics and artificial intelligence, micro-satellites etc. Embedded systems with integrated designs for surveillance, information gathering, assimilation and analysis leading to efficient decision-making, will be vital to success in the rapidly changing environment of the future. Integrated defence planning involving all stake-holders in India's future, including Indian industry, will thus be the key to India's defence and security in future.

Politics of Nuclear Weapons and International Affairs: Indian Perspective

The pursuit of NW in the US during World War II was driven by the urgency of acquiring ultimate techno-military superiority for decisive victory in the long war. While the weapon tests were underway in total secrecy in the US laboratories and deserts, the decision to use the weapon on Japan was perhaps in response to the humiliating Japanese attack on Pearl Harbour. One wonders if Japanese intelligence had any inkling of the NW development, and if so, whether the Pearl Harbour attack plans would have been aborted. The first ever atomic bomb 'Little Boy' (a 10 Kilo-Ton Uranium Bomb) dropped over

Hiroshima on August 6, 1945 killed over 70,000 and injured an equal number in a matter of minutes. Three days later, the second bomb 'Fat Man'—a more powerful Plutonium bomb, killed over 390,000 and injured an even higher number. Japan surrendered immediately to end World War II. This was the defining event that demonstrated the devastating and hence, decisive impact of technology in international affairs.

> On July 16, 1945, in a white blaze that lit-up the northern New Mexico-dark skies, the first nuclear weapon test ushered in the Atomic Age. The light of the explosion turned orange as the atomic fireball began shooting upwards at 360 feet per second, reddening and pulsing as it cooled. As the characteristic mushroom cloud of radioactive vapour materialized at 30,000 feet high, beneath the cloud, all that remained of the soil at the blast site were fragments of jade green radioactive glass created by the heat of the reaction. The brilliant light from the detonation pierced the early morning skies with such intensity that residents from a faraway neighbouring community would swear that the sun came up twice that day!
>
> Upon witnessing the explosion its creators had mixed reactions. They felt as if the equilibrium in nature had been upset.
>
> Robert Oppenheimer, though ecstatic about the success of the project, quoted a remembered fragment from the Bhagavad Gita. "I am become Death," he said, "the destroyer of worlds."
>
> *(https://en.wikipedia.org/wiki/J.Robert_Oppenheimer)*

After witnessing the horrors of Hiroshima and Nagasaki in August 1945, it was very clear that NW would serve very effectively as the ultimate deterrent to war designs against a Nuclear Weapon State (NWS). The Soviets soon acquired the same NW by 1949, with the UK and France conducting their NW tests in 1952 and 1960 respectively. This was the start of the new age of nuclear deterrence that spurred R&D for more powerful weapons, long range bombers and guided missiles for extending the range and enhancing the effectiveness of nuclear deterrence world-wide.

The prospect of such powerful weapons spreading to other countries, was however too dangerous and the world community, including scientists responsible for NW development, raised their voices for elimination of NW. However, both the US and the erstwhile Union of Soviet Socialist Republics (USSR) continued with their pursuit of more powerful NW designs, and by 1955, the vastly more powerful thermo-nuclear weapon, better known as the 'Hydrogen Bomb', was developed by both the superpowers, with others like Britain, France and China following soon.

Concerns about nuclear war brought together an informal group of influential scholars and scientists like Bertrand Russell and Albert Einstein, to start the 'Pugwash' movement in 1955, for reducing the danger of NW by seeking cooperative solutions. Over 200 Pugwash conferences to date have made valuable contribution towards spreading the awareness of nuclear disarmament for global peace. This was duly recognised with the award of the Nobel Peace Prize to the Pugwash movement in 1995. [15]

The early 1960s were witness to atmospheric testing of these mega-ton class Hydrogen bombs that created serious weather disturbances. Fortunately, a Partial Test Ban Treaty (PTBT), conceptualised by Japan and India was agreed to by the NWS in 1963, to put an end to atmospheric testing. Meanwhile, China established the capability of NW with its own nuclear test in 1964, to claim its right to be among the first batch of NWS.

By 1967, the five NWS decided to form the famous 'London Club' to prevent further proliferation of NW technology. This was the genesis of the NPT that was opened for signature in 1970. NPT mandated that the five NWS would not assist any another country in developing NW and prevent proliferation of NW technology through tight technology controls. France and China were party to NPT in principle, but signed it only in 1992.[16]

NPT was the first international treaty, signed by over 187 nation-states that legitimised NW for the five members of the 'London Club', while all other signatories pledged to remain non-NWS. The five NWS were mandated not only to prevent NW proliferation, but were also committed to work towards nuclear disarmament, leading to the ultimate elimination of NW. The NPT came into force in September 1970 for a period of 25 years, with a major review in 1995, to ascertain if its major objectives were achieved. As is well known, NW proliferated vertically within the five NWS to huge total numbers, with scant regard for disarmament and by the start of the 21st century, the world grudgingly accepted failure of the NPT to over-ride political priorities, that led to eight States having NW.

It is worth noting that the importance of nuclear technology for other attractive applications such as nuclear energy generation and for Electromagnetic Pulse (EMP) effect were established fairly early and hence, many countries wanted to acquire this very versatile nuclear technology. Therefore the International Atomic Energy Agency (IAEA)[17] was established

to monitor all nuclear activities to ensure that the NPT guidelines are followed by all nations, and also to encourage cooperation for peaceful application. IAEA was given international powers under the aegis of the United Nations (UN), but it had no role to monitor or report on the commitment of the five NWS towards voluntary disarmament and eventual elimination of NW. As a result, pursuit of NW continued unabated during all the years of the cold war, leading to stockpiles of over 20,000 NW that could annihilate humanity many times over.

Most non-NWS signed the NPT with the assurance from the NWS leaders that they would be protected in the event of any possible nuclear attack. Israel, India and Pakistan were the exceptions that did not join the NPT as non-NWS for different reasons. Israel presumably had NW by the late 1960s (with tacit US help) but it did not want to declare this overtly, to avoid any nuclear arms race in the region. India rejected the NPT because of its discriminatory nature and to keep its nuclear options open, due to the grave security concerns from nuclear-armed China. Pakistan did not sign the NPT because its sworn single enemy, India did not sign the NPT. Much of this is history and widely discussed in open domain literature.[18]

What deserves special mention is that the Indian policy of not joining NPT was often fiercely contested at international forums but India stoically maintained its sovereign stand while developing nuclear technology, primarily for energy needs, but also for possible exigencies of national security. Serious national security concerns forced India in 1971 to launch military action to liberate East Pakistan and for the creation of independent Bangladesh that was expected to be a friendly neighbour. This however, prompted Pakistan to declare its determination to challenge Indian regional superiority by acquiring NW by whatever means. This was the beginning of a nexus evolving between Pakistan and China that eventually helped Pakistan to acquire NW.

It was in the face of this combined threat from adversarial neighbours that India carried out a PNE in 1974, as a diplomatic confirmation of its deterrence capability, using indigenous nuclear technology capability. This led to a major international outcry and serious technology embargo against India by the Western alliance of advanced countries. The NSG was created to restrict the supply of any nuclear technology to India and the Zangger's List was drawn up to specify all items to be denied to non-allies under strict export controls. The embargo did slow down India in its pursuit of nuclear technology even for energy purposes, but it also spurred India to pursue indigenous R&D to acquire most critical technologies. Meanwhile, India with its own ideological

preference for nuclear non-proliferation, demonstrated exemplary restraint in nuclear-missile matters and other sensitive technologies.

India, Israel and Pakistan who refrained from signing the NPT, now possess NW and are thus de-facto NWS. North Korea acceded to the NPT but announced its withdrawal in 2003 to conduct some questionable nuclear tests. Countries like Argentina, Brazil and South Africa ended their NW programmes and joined the NPT as non-NWS in the 1990s. Others like Ukraine, Belarus, and Kazakhstan gave up former Soviet NW on their territories and joined the NPT as non-NWS in the 1990s. Iraq was suspected to have a NW programme prior to the 1991 Gulf War but UN inspectors subsequently oversaw the programme's dismantlement. Libya gave up a clandestine NW programme after a 2003 agreement, and Syria was also suspected to have a clandestine WMD programme. Iran was found to be non-compliant with its NPT commitment, but it claimed that its nuclear objectives were entirely peaceful. US led international negotiations are in progress to ensure that Iran does not acquire capability to have its own NW because it would be a direct threat to Israel.

The decade of the 1990s proved to be quite eventful for the NPT regime and politics of NW. The end of the cold war prompted a relook at the huge stockpiles of NW between US and Russia and the unnecessary cost of maintaining them. While this led to a fresh impetus to disarmament under the Strategic Arms Reduction Treaty (START), negotiations began for other avenues for nuclear disbarment—the CTBT and the Fissile Material Cut-off Treaty (FMCT). The idea was to use the 25-year NPT review in 1995, for major initiatives in universal nuclear disarmament. Unfortunately, the process instead became an arms control exercise to perpetuate the discrimination between the nuclear haves and have-nots. China and France hurriedly conducted additional nuclear tests before the 1995 NPT review conference decided to ban future testing, but India was denied the opportunity, despite the genuine threat to its national security from nuclear capable neighbours on either side with a history of wars.

Despite enormous international pressures, India conducted itself with wisdom and grace at the CD in opposing the indefinite extension of the highly discriminatory NPT, and also declined to sign the CTBT to preserve its right to NW if deemed desirable, in keeping with its supreme national security interests. In May 1988, India finally decided to carry out a series of nuclear

tests to declare itself a NWS. A good account of these historical proceedings can be found in Bharat Karnad's book.[19]

The 1990s saw India project its nuclear priorities with a very mature and decisive foreign policy, and Indian diplomats armed with technological information and clear national priorities performed admirably in international affairs. After the initial adverse reaction to India's nuclear tests and the concomitant sanctions by the Western alliance of nations, the realities of geopolitics prevailed in the long-term, and by 2005 nuclear India won recognition of the international community as a progressive and responsible nation worthy of nuclear technology cooperation. By 2008, the Indo-US civil nuclear cooperation agreement was finalised to usher in a new era for India, transforming it as a global partner in nuclear technology and no more a target of the non-proliferation community. In exchange, India revised its export control laws to be at par with international standards and separated its civil nuclear activities to be put under IAEA safeguards, so that India was cleared to enhance its nuclear energy capacities.[20]

Since the indefinite extension of the NPT in 1995, there have been periodic NPT Review Conferences (Rev-Cons) every five years and the last Rev-Con in May 2010 re-asserted the importance of international commitment to non-proliferation through renewed focus on the CTBT and the FMCT that have yet to find international consensus on all the aspects. Although US-Russia dialogue on nuclear disarmament has resulted in a reduced stockpile of NW in both countries, there are several complex issues that are yet to be resolved, without which complete disarmament may not be possible. The US has itself been reluctant about signing the CTBT due to its own revised national security perceptions, and the FMCT remains mired in disputes about cut-off definitions etc.

Nuclear Deterrence—Past, Present and Future

International balance of power equations in the past 4-5 decades have evolved, with a very dominant influence of nuclear-missile deterrence, and for most of the developed economies, the probability of a major war is reduced significantly. But for developing regions with NWS, nuclear deterrence continues to play an important role in the security matrix. Future decades however, may be quite different, dictated not just by nuclear deterrence, but also by other forms of techno-economic deterrence and changing security perceptions. The world is changing in many dramatic ways and the technology

revolution has created many new capabilities that can provide potential deterrence effects for changing patterns of threat.

In the unequal but interdependent world of today, while economic sanctions and techno-military coercive diplomacy are acquiring significant deterrence value, unprecedented advances in technology capabilities, combined with knowledge and innovation capacities in outer space and cyber space are creating a new class of non-nuclear deterrence options. The analysis of the future impact of ICT and artificial intelligence on international equations can also help in appreciation of the limitation of traditional nuclear-missile deterrence in future. It is this realisation that is forcing modern human society to seriously re-consider the future of nuclear deterrence and the prospects of a world free of NW.

Since deterrence is intrinsically linked to threat perceptions of both the parties involved, it is relevant to examine the changing patterns of threat perceptions and their impact on the interplay of deterrence. For most of the progressive world today, the main threat is perceived from non-state or trans-national actors and from irresponsible rogue States that may support such entities for political objectives. Threat perceptions are now more about dangers to human life or civil society and not so much in terms of the sovereignty of States which is now difficult to challenge. Thus, major security concerns of the future may increasingly include economic security, water and food security, energy security and environmental security—areas where nuclear deterrence cannot work.

However, conflicts among nations or societies, as well as military threats to national security, may remain a reality of life and hence, some form of deterrence, a mechanism of making the adversary mortally afraid of punitive retaliation will continue to be relevant. As of today, NW still remain the ultimate weapons and those in possession of NW are unwilling or unable to dilute their dependence on them.

With the focus of nuclear deterrence shifting to Asia and West Asia, competing demands of development and security may play out differently in the developing regions. It is now internationally perceived that Asian nuclear powers may have to stabilise the nuclear deterrence parameters soon, and are therefore compelled to negotiate peace with greater realism than before. At the same time, any adventurism of failing or rogue States such as North Korea or Pakistan with NW capability can rejuvenate the importance of NW in affected regions. If the international security scenario deteriorates significantly

and compels additional countries to acquire NW, that would be a major blow to nuclear non-proliferation goals, and create serious impediments to the future of nuclear disarmament. Any escalation of conflict between major powers can potentially take the deterrence-stability calculus to different dimensions including outer space, cyber space and even use of the environment as a weapon.

Since 9/11, the security focus of the US and most other progressive nations has shifted to homeland security on issues of how to prevent terrorist strikes and prevent terrorist organisations or rogue States from acquiring Biological-Chemical-Nuclear-Radiological (BCNR) weapons. This indicates a shift in threat perceptions from a possible nuclear war, to the clandestine use of WMD technology for asymmetric warfare. Technologies of situational awareness and preventive counter measures, such as remote use of combat UAVs, are proving to have more practical deterrence effect than NW.

At the same time, energy or water shortages and global warming-induced climate change are very serious issues of global dimension, that would demand serious international cooperation, and if that fails, it could cause future wars, where the nuclear-missile deterrence of a particular nation or group of nations would have little relevance. Clearly, future peace and stability will demand a more mature cooperative security approach by all progressive nations, both at the regional as well as global level. It is pity that while technology and development are pushing mankind to cooperation and peaceful co-existence, fundamentalism is reducing tolerance and increasing violence.

It is in this backdrop of changing security dynamics that 'minimum deterrence' is emerging as the preferred choice for many NWS. Nuclear weapons have changed the relationship between war and politics in a way that makes nuclear war un-winnable even for an aggressor. And yet, an otherwise weak or unstable military regime may regard NW as usable weapons and dangerously lower the nuclear threshold as is happening with Pakistan developing tactical NW.

This inherent contradiction is perhaps the rationale for a 'minimum posture' that is based on how few weapons may be adequate to have effective deterrence to avoid any escalating tension between nuclear adversaries. As analysed by Jeffrey Lewis, "A strong case could be made for the idea that a policy maker sane-enough to be deterred in the first place is unlikely to consult force exchange ratios or find comfort in strategic superiority when contemplating a nuclear war."[21]

If the above logic of minimum deterrence prevails, it could well set the stage for serious nuclear disarmament initiatives. However, the perceptions of minimum deterrence are very diverse and the margins of definitions too wide for setting any universal benchmarks. Deterrence is also a dynamic concept that must be responsive to changing strategic environment—for example, changes in political alignments or changes due to an effective missile defence shield or any decisive future technology capabilities can change deterrence dynamics. Hence, the NW strategy for different nations or different regions will always be different. Of late, there is also growing apprehension that if irresponsible rogue States and/or terrorist organisations get access to nuclear or radiological weapons, the likelihood of their being used may be far more real. This complicates the calculations for minimum deterrence and hence the reliance on nuclear deterrence would continue to be important in the foreseeable future.

Minimum deterrence is a choice for a possessor of NW that offers adequate deterrence at an affordable cost without unduly provoking the adversary. This is the rationale for India's nuclear doctrine of credible minimum deterrence that is meant to be credible for the adversary and the 'no-first use' posture is to signal a strong preference against any nuclear war-fighting. The doctrine of credible minimum deterrence and 'no-first-use' also allows India to gain deterrence at a low cost and be seen as a mature nation that has no intention of using NW except for retaliation after enemy strike. However, the doctrine demands survivability of first strike by the enemy and a capability of massive retaliation against the aggressor. India clearly does not want to have a nuclear war with anyone. But a well articulated nuclear posture is necessary to gain maximum deterrence benefit.

Credible minimum deterrence thus relates to the lowest level of assured damage to prevent nuclear aggression or attack, with the least number of NW possible. What deters is not one's own certainty of inflicting damage, but the adversary's perception of the potential risk. Hence, beyond a point, neither the number of weapons nor the technological sophistication actually matter. In context of the India-Pakistan situation, a more dilute form of recessed deterrence seems to have worked so far, where the weapon is not mated to the delivery system (missile) to minimise accidental panic or unauthorised use. This represents a very mature approach to nuclear deterrence, best suited for the ultimate universal goal of having a nuclear-free world. There are thus lessons that other NWS can learn from the South Asian model of credible minimum nuclear deterrence.

Future Technology Trends and Impact on Balance of Power Equations

Modern armed forces always face the challenge of dealing with present threats while preparing for tomorrow's wars. Since each challenge has its own share of uncertainties, the priority is always to find how best to avoid a war without compromising one's absolute core national security priorities. The process is very complex and dynamic, demanding broad background knowledge of defence technology potential and also very reliable situational awareness of the security environment in all dimensions. This can be well appreciated from a quick look at the global leadership in defence technology. The US forces are concentrating on the immediate goal of winning the global war on terrorism while also transforming US techno-military power to levels that can ensure continued US supremacy in global affairs. In the final analysis, strong defence capability will be increasingly dependent on technological sophistication and achieving technology leadership will require significant economic strength. As is well known, technology is one of the main tools for economic competitiveness. It is in this context that technology trends will have a major impact on global affairs in the future.

The rapidly globalising world today is going through a unique transformational phase where the very premise of future conflicts and future wars is being re-defined. There is an overall appreciation that, probability of conventional full-scale war between major powers is getting very low and real conflicts between major States in future would be about sharing energy resources, about level playing fields for economic competition and about environmental degradation and global warming issues that can have a very profound security and economic impact in the future. Therefore, the increasing gap between the haves and have-nots, will probably be the major cause of tension among nations. Fortunately, the deterrence value of high-technology for avoiding war is shifting away from NW with every new maturing technology and the future world power equations will be decided more by techno-economic capabilities rather than by the mere might of military hardware and weapon systems. Cost of war no matter who wins, has gone up very high and even cost of maintaining large forces is becoming difficult to afford for any country. Hence, lower cost technological means are bound to win in the long run.

However, ideological or religious divide may continue to be a nagging problem and regional conflicts or religious extremism may remain unresolved in many parts of the world. Hence, States involved in such circumstances

will continue to remain sensitive to conventional military strengths and must be prepared for possible short armed conflicts or sustained guerrilla wars. The information revolution has transformed the level of awareness in the world and we now have a peculiar mix of expectations and aspirations among developing and progressive nations. For them, pursuit of cutting-edge technologies for rapid economic progress has become top priority, while at the same time they cannot neglect older proven defence technologies and weapon systems for regional conflicts.

Therefore, techno-military supremacy continues to remain as important as ever and even the most powerful nations remain focused on retaining a techno-military edge over immediate adversaries and competitors. The recent history of use of military force to bring-about a change of regime in Iraq and the emerging acceptance of the legitimacy of a preventive military strike, indicate a new trend in re-shaping global perceptions of use of military power and risk reduction measures using the latest in technology. Another clear emerging pattern is the nature of asymmetric threat, which may dictate the technological capabilities needed for the future to contain them, and the global cooperation imperatives for sharing such technologies among peace-loving nations.

The evolution of military technology can be well understood from the marked difference in technological sophistication and strategies of the superpower nations and that of other lesser powers in the developing world. Looking into the future for relevant technologies and capabilities for a nation will naturally be influenced by the associated maturity of the nations in the overall world power matrix. However, given the interdependent nature of the modern world, regional issues may have unexpected bearing on world events in the future and hence, global security and stability concerns will have many layers of uncertainty that the future defence forces and diplomats managing international affairs will have to address.

Any future predictions on complex issues such as conflicts and the attendant war-fighting responses required, will always run the risk of being wrong; and yet predictive thinking is essential to long term perspective planning. One approach could be based on scenario building to provide some measure of cause-effect logic to futuristic projections. Looking at the world beyond 2030, several situations could be indicative of probable scenarios.

- We may well have a world split into two unequal camps: a small, wealthy, technologically advanced and politically stable minority group

of nations, and the large sections of poor, backward, sick, resource-starved majority that will remain unstable. Technology and power would determine trends in both the directions, in either relative narrowing or further widening of the divided world.

- A world of rampant nationalism with State and/or non-state-sponsored terrorism with fluid coalitions among them. Transnational threats, territorialism, strong national sentiments, proliferation of refugees and authoritarian means of governance would flourish. Probability of multiple regional conflicts could be high and major powers could remain involved in counter-terrorism and humanitarian assistance as well as peacekeeping operations.
- By 2030, the Asian Century may be well established with power, prestige and techno-economic capability. Economic, technological and political influence of this region could lead to unknown responses from present major powers that are not used to being less powerful, leading to new tensions and uncertainties. The technological edge of the Western alliance and economic powers and the human potential of Asia could either combine for greater world peace or could work against each other.
- One may well have a world where technology may advance exponentially and proliferate widely, where multinational corporations dominate international affairs and loosely cooperate in a syndicate mode. Economic competitiveness and profits would be the dominant concerns, while conflicts may be dealt with through proxies. The challenge to democratic countries with old-style values would be to maintain their relevance and competence in a new world, demanding a whole new approach to security and defence.
- A business-as-usual scenario in which events and equations would evolve slowly, adjusting to real-time changes. Most nations would focus on internal stability and progress and would not stir-up world peace with a delicately balanced sense of stability. Political awareness and techno-military capabilities will have to be on high alert for unknown threats.

In reality, the actual situation may be a mix of two or more scenarios above and the demand for technologies and defence systems for the future would be dictated by the comprehensive threat perceptions as well as the requirements of the power projections of individual States.[22]

Future Trends

As we commenced the 21st century, a technology driven revolution in global affairs was perceived to be occurring, largely due to the infusion of ICT in planning, execution and monitoring of politico-military activities of advanced countries. Something similar was happening in the defence technology field, where trends indicated that technologies for space-based capabilities such as cyber security, nanotech or biotech-enabled new capabilities—to contribute to the next RMA—in turn could have a major impact on international affairs. Some manifestations of these advances would certainly include advanced robotics with bioelectronics and cognitive intelligence, nano-materials, directed energy systems and advanced networks for global governance. The outlook is for the rapid evolution of new technologies eventually leading to the development of several advanced defence capabilities and a system-of-systems approach that will take advantage of the cumulative effect of employing each of the new capabilities simultaneously and in proper synchronisation.

For conventional warfare, future trends indicate four potential major warfare scenarios—long-range precision strike, electronic/information warfare, space warfare and dominating or pre-emptive manoeuvres. Of these, precision strike is the most developed technology and intense R&D work is being done in the area of information and electronics warfare. A comprehensive understanding of space warfare and the full scope of dominating manoeuvres will need more analysis for optimal planning of politico-military objectives in the future. A high-precision strike with advanced non-nuclear warheads will be able to achieve effects similar to a NW strike, but without the attendant risk of escalation to intolerable levels of mutual destruction. When directed against targets comprising the enemy nerve centre, a precision strike itself can prove very punishing to offer deterrence value. Integrating the three components—precision strike, electronic warfare and dominating manoeuvres—will likely comprise the very potent next RMA unfolding presently.

Modern battlefields today have significantly advanced use of electronics, optoelectronics, radars, computers etc. to fully exploit technology to achieve a digital battlefield advantage, with its unique features of real-time situational awareness and battlefield transparency. Multispectral sensors from land, sea, air and outer space platforms, the all-weather day-night C4ISR capabilities and the network-centric strategies will be crucial for advanced battlefield capabilities. Technology sophistication of each component, the high cost of

systems and the efficacy of integration will determine the extent to which a country can achieve true digital battlefield advantages.

Cyber space is becoming the nervous system hub for all military and economic activities and hence cyber security will be vital to all strategic as well as tactical considerations. The speed and anonymity of a cyber attack makes it very difficult to distinguish between the actions of terrorists, criminals and nation-states. Electronic warfare would thus gain significant importance in the modern battlefield. On the one hand, sensor technology integrated with ICT would add unprecedented capabilities and on the other, the vulnerabilities of systems to ECM and ECCM will get compounded. The challenges are enormous, going beyond mere technologies to standards, practices, software protocols and international coordination needs that are yet to be understood fully. The increasing use of electro-magnetic spectrum across national boundaries will require new approaches to international dialogue, for creating win-win situations for all peaceful and progressive nations.

At the national level, information warfare could be viewed as a new form of strategic warfare, wherein one of the key issues is vulnerability of socio-economic systems and the question will be—how to attack the enemy's system while protecting one's own. At the military operational level, information warfare may contribute to major changes in the conduct of warfare. Hence, one of the key issues will be the vulnerability of command, control, communications, and intelligence systems in conflict situations. Information technology is making distributed systems commonplace and virtual organisations are growing like new cultures. The rapid rate of growth of these types of new organisational entities would seem to suggest strengths that the future military will have to counter with new technologies and strategies. Issues of global governance may emerge as the main challenge for diplomats and foreign policy experts in future.

Missile defence technologies are becoming increasingly important for most countries, largely due to continued proliferation of low-end missiles, as well as due to technology sophistication of cruise missiles, that have proved very effective from stand-off ranges. Concerns about unexpected attacks from terrorist groups have further sharpened the need for effective early warning technology, as well as quick reaction hypersonic missile defence systems for defence against surprise attacks. The future will certainly witness a wider spread of missiles of all types around the world because the Missile Technology Control Regime configured during the height of cold war has become

increasingly irrelevant in the atmosphere of inevitable technology diffusion happening in the globalising world. Given the high cost of technology sophistication, the need to seek international cooperation for missile defence technology among a group of friendly nations, has replaced the urgency of controlling missile proliferation. Instead, the trends indicate that focus is shifting to achieving better range, flexibility and accuracy for missile defence systems that can deprive the enemy of the deterrence value of ballistic missile attack. These techno-economic perspectives are creating new challenges for the future of diplomacy, towards building common capacities against common threats, such as from extremist groups.

As lethal or dangerous capabilities of modern technology continue to increase, the need to curb misuse of such technologies becomes more urgent. It is important to note that there is significant universal consensus against the use or threat of use of biological and chemical weapons, and the Biological and Toxin Weapons Convention was signed in 1972 by over 170 countries. Nevertheless, many countries have continued with such bio-weapons' R&D under the justification of developing defence against such weapons. Hence, several biological warfare agents have been under development by most major powers and the ban is based more on ethical values that technological constraints. Biological weapons perhaps constitute the lowest cost WMD that can have devastating effects on the human population almost comparable to NW. It is thus easy to understand that bio-weapons are very attractive for non-state entities and in the present context the threat of bio-warfare has gradually changed to a threat of bio-terrorism. The subject is very complex and alive in the security calculus of most nations—a clear demonstration of how lethal technology in wrong hands can have very grave impact on international affairs. Any reader interested in further details may find the book, *Bio-Weapons: The Genie in the Bottle* very interesting and informative.[23]

The impossibility of putting the 'Genie' of WMD technology in the bottle may be one reason why NW continue to enjoy the active patronage of most NWS who are in fact the most powerful nations on earth. It is believed that the US may be working on the next generation of more effective tactical weapons and hence, the threat of WMD and their delivery vehicles will be real and persistent for many nations. In addition, there is fear of another kind of WMD—Weapons of Mass Disruption—such as EMP devices that can paralyse electronics and communication infrastructure. While advanced nations are designing compact and efficient EMP weapons and microwave

weapons, the thirst for technologies that can provide protection from such advanced weapons will continue to grow.

Directed energy weapons using high-power laser technology have achieved significant maturity in the past few decades, to provide a new capability for missile defence, as well as for possible future space warfare.[24] Despite many hurdles, the US Air Force project on the Airborne Laser has demonstrated unprecedented capability for aerospace dominance. Such high-altitude aerospace capabilities can decisively destroy enemy missiles or satellites in a matter of seconds, high above the atmosphere, with the common man on the street being totally oblivious to the far reaching consequences of such manoeuvres.

As the technological sophistication of these directed energy weapon systems improves, the efficacy of multi-role deployment will increase and the cost considerations will become more acceptable. As it is, the US-Israel joint project on ground-based laser defence against low-flying attack has proved fairly successful and technology is being pushed for short-range point defence of high-value assets such as command centres. An advanced version of the Space-Based High Energy Laser System would be a space-based, multi-megawatt, high-energy laser constellation that can operate in several modes. In its weapon-mode it can attack ground, air, and space targets and destroy them with energy beams in a matter of seconds. In its surveillance mode, it can operate with low power for active illumination imaging or with the laser inoperative, for passive imaging. World-wide coverage could be provided by a constellation of 15-20 High Energy Lasers. The system provides counter-space, force application and even weather modification applications. It is natural for all progressive nations to want to pursue such revolutionary new technology, but these are very sophisticated, multi-disciplinary and expensive systems that only a few major powers can afford and maintain.

Unmanned Combat Air Vehicles: In recent times, the world has been witness to the US' use of UCAVs in its war against terror, for precision attacks on specific small-size targets in enemy territory. How far this new technology gets extended for regional conflicts is yet to be clear. But such extended reach without physical human encroachment in areas of conflict or dispute, would certainly create major challenges for the diplomatic community world over, and it might be required to establish new norms of engagement using robotics technology in war situations in the future. Advanced UCAVs in the future can loiter at high altitude over the region of interest for long periods of time (over 24 hours) until called upon to strike a target. It could carry a suite of

multispectral sensors (optical, infra-red, radar, laser, etc.) and supply information to its suite of standoff precision-guided munitions. While in its subsonic loitering mode, it would be designed to operate at very high altitudes over the region of interest, for extended periods of time without refuelling. This would be very useful for surveillance and reconnaissance missions for the Global Information Management System (GIMS) of the host nation or a group of nations. On a secondary mission, it could also perform ECM and ECCM roles.

Attack Microbots: Attack Microbots are a class of highly miniaturised (millimetre scale) electro-mechanical systems capable of being deployed en-masse, and perform individually or collectively for various missions, including target reconnaissance and destruction. Various deployment approaches are possible, including dispersal as an aerosol, transportation by a larger platform and full flying and crawling autonomy. Attack is accomplished by a variety of robotic effectors, electromagnetic measures or energetic materials. Some sensor microbots' capabilities would also be designed for target analysis. Microbots could provide unobtrusive, pervasive intervention into adversary environments and systems. The extremely small size would provide high penetration and natural stealth features.

Single-Stage-to-Orbit Trans-Atmospheric-Vehicles: Trans Atmospheric Vehicle (TAV) systems could provide space support and global reach from the earth's surface to low earth orbit (LEO) using a combination of rocket and hypersonic air breathing technology. The trans-atmospheric vehicle of the future would take off vertically, could be re-fuelled in either air or space, and would have capability to land on a conventional runway. Designed for variable payload capacity (up to 10,000 lb) it would perform both as a sensor and a weapons platform. Alternate missions may include deployment and retrieval of micro-satellites from LEO and possible deployment of anti-satellite (ASAT) weapons. The US Air Force-sponsored Spy-plane X-37B discussed in chapter four of this book is a clear example of the direction the technology is taking.

Antimatter Weapons: The US Air Force is believed to be investigating ways to use a radical power source—antimatter, in future weapons. Antimatter is a term normally heard in science fiction, but it can actually exist in laboratories, and has been intensively studied by physicists over the decades. Every type of subatomic particle has its antimatter counterpart, and when matter and antimatter collide, they annihilate each other in an immense burst of energy.

Thus, positron energy conversion could be a revolutionary energy source that may enable realisation of antimatter bombs small enough to hold in hand, and perhaps power engines for 24×7 surveillance aircraft. More cataclysmic possible uses may include, a new generation of super weapons—either pure antimatter bombs or antimatter-triggered NW, or antimatter-powered EMP weapons, that could fry an enemy's electric power grid and communications networks. Such technologies on the fringe of science fiction continue to be in the realm of wishful capabilities, due to unacceptable technological costs, and some unanswered questions of practical viability and ethics of use. But these are already potential proven technologies that are capable of creating yet another RMA in the future.

Priorities for India

For India with long coastlines and land borders, conventional military capabilities will continue to be important for the foreseeable future. In addition, the armed forces will also have to be prepared to combat insurgency and terrorism being fuelled by adversarial States. The proxy war of low intensity is fairly unique to India, and specific technologies for fighting such low intensity conflicts with non-lethal weapons will need major attention. Much like modern conventional war-fighting, reaction time needs to be reduced for enhanced effectiveness. Military modernisation in India for the immediate future will have to concentrate on enhanced use of UAVs for reconnaissance and combat use of multispectral sensors and data fusion, better signal processing technology, hypersonic missile technology, and military satellite systems. PGMs, enhanced underwater technology and energy beam technologies may provide the much desired decisive regional superiority for India.

For short border conflicts, India will have to acquire robust early warning systems with C^4ISR integration to move towards 'network-centric' strategies. While the navy will have to focus more on littoral warfare rather than blue water capabilities, the air force will need to establish clear dominance in its sphere of influence, with day and night precision strike capability. There is urgent need to mobilise space assets for better surveillance and coordination of integrated operations. Missiles and missile defence technology will have to keep pace with the developments in the world. Indigenous capabilities will be crucial in the areas of electronic warfare, missile defence technologies, DEWs and satellite defence, as these critical technologies will always be vulnerable to technology controls by supplier nations.

Finally, India's nuclear doctrine of credible minimum deterrence and no-first-use posture presents a unique set of challenges for the strategic planners and diplomats. Since India continues to advocate total nuclear disarmament by all nations, and does not support the logic of large-scale stockpiling of weapons, India must rely more on deterrence value from non-nuclear technology superiority over the adversary. At the same time, it will be imperative to be alert to any adventurism with WMD in the neighbourhood and hence, a well-organised civil defence mechanism along with an efficient emergency disaster management system will be crucial. For India, the real challenge in the next few decades will be to manage large-scale demands of the armed forces for national security, while attempting to stay ahead in economic competition, to achieve a leadership role in global affairs. Technology and diplomacy must therefore join hands to achieve this.

NOTES

1. Amitav Mallik, *Technology and Security in the 21st Century: A Demand-Side Perspective*, SIPRI Research Report No. 20, Oxford University Press, New York, 2004, p. 131.
2. India conducted its first nuclear detonation, described as a 'peaceful nuclear explosion (PNE), on May 18, 1974. It was code-named 'Smiling Buddha'. At www.fas.org/nuke/guide/india/nuke/first-pix.htm (Accessed June13, 2014).
3. Government of India took a bold step in the year 1988 to create a new office of 'Adviser, Defence Technology' at Embassy of India in Washington D.C. to negotiate and reverse technology denial decisions by U.S. against India.
4. The Indian representative at the Conference on Disarmament argued that the "CTBT that we see emerging appears to be shaped more by the technological preferences of the Nuclear Weapon States rather than the imperatives of nuclear disarmament. This cannot be the CTBT that India can be expected to accept". See Manpreet Sethi, "CTBT and India's Options" at www.idsa-india.org/an-sept3-00.html (Accessed May 7, 2014).
5. Pokhran-II was codenamed 'Shakti'. With the series of nuclear tests in May 1998, India announced its claim to be a Nuclear Weapon State. See www.southasiaanalysis.org/paper690 (Accessed May 7, 2014).
6. "The Kargil Review Committee headed by veteran security analyst K. Subrahmanyam produced its report in record time and this was submitted to the… government." See C. Uday Bhaskar, 'Kargil: Whose war was that?', *India Strategic*, August 2009 at www.indiastrategic.in/topstories365.htm (Accessed May 7, 2014).
7. See Mark Hibbs, "Moving Forward on the U.S.-India Nuclear Deal", *CIEP*, April 5, 2010, at www.carnegieendowment.org/2010/04/05/moving...india-nuclear-deal/25yl (Accessed May 7, 2014).
8. Sachin Kumar, "Modernisation Plan of the Indian Navy", *NavalJourney.com*, December 19, 2013, at http://navaljourney.com/modernization-plan-of-the-indian-navy/ (Accessed May 7, 2014).
9. "Indigenous nuclear submarine heads sea trials", *Times of India*, December 13, 2014, at www.timesofindia.indiatimes.com/india/submarine.Arihant. (Accessed Dec 21, 2014).
10. Laxman Kumar Behera, "Modernisation of the Indian Air Force", *Defence Review Asia*,

January 17, 2013, at http://www.defencereviewasia.com/articles/200/Modernisation-of-the-Indian-Air-Force (Accessed May 7, 2014).

11. For details see "BrahMos Supersonic Cruise Missile, India", Army-technology.com at www.army-technology.com/projects/brahmossupersoniccru/ (Accessed May 7, 2014).
12. "It was an incredible year for India's missile scientists", See *A Summary of Indian Missiles Development in 2012*, *Missile Threat,* January 2, 2013, at http://missilethreat.com/a-summary-of-indian-missiles-development-in-2012/ (Accessed May 7, 2014).
13. "India launches five foreign satellites", *BBC News,* June 30, 2014. See www.bbc.com/news/world-asia-india-28083893 (Accessed May 7, 2014).
14. *Space Security—Need for a Proactive Approach: Report of the IDSA-Indian Pugwash Society Working Group on Space Security*, IDSA and Academic Foundation, 2009.
15. "Pugwash Conferences on Science and World Affairs is an international pacifist organization bringing together scholars and public figures in order to reduce the threat of wars, nuclear dangers, and to seek peaceful resolutions to all international conflicts." See Pugwash Conferences on Science and World Affairs at www.nobelforpeace- summits.org/.../pugwash-conferences-science-world. (Accessed May 8, 2014).
16. Treaty on the 'Non-Proliferation of Nuclear Weapons' (NPT). Text of the Treaty. United Nations Office for Disarmament Affairs, at www.un.org/disarmament/WMD/Nuclear/NPTtext (Accessed May 8, 2014).
17. International Atomic Energy Agency," Nuclear Safety and Security". See www-ns.iaea.org/security (Accessed June 8, 2014).
18. Andrew Koch, "India, Pakistan: nuclear arms race gets off to a slow start", *Jane's Intelligence Review*, Vol. 13, No. 1, 2001, at http://hufind.huji.ac.il/Record/HUJ001326049 (Accessed May 8, 2014).
19. Bharat Karnad*, India's Nuclear Policy*, Praeger Security International, Westport, CT and London, 2008.
20. Amitav Mallik, "US-India Nuclear deal—Nuke numbers: deal adds up", Op Ed.. *Indian Express,* August 17 2006, at http://archive.indianexpress.com/news/nuke-numbers-deal-adds-up————/10751/ (Accessed May 8, 2014).
21. Jeffrey G. Lewis, "Beyond that minimum threshold, nuclear weapons provide little additional deterrent benefit", at lewis.armscontrolwonk.com/archive/1936/minimum-deterrence (Accessed Dec 21, 2014).
22. Rajiv Kumar, The National Interest Project, Indian Council for Research on International Economic Relations, December 2010. (Accessed May 8, 2014 from personal notes).
23. Ajey Lele, *Bio Weapons: The Genie in the Bottle*, Lancer Publishers, 2004.
24. Amitav Mallik, *High Power Lasers—Directed Energy Weapons: Impact on Defence and Security*, DRDO Monographs/Special Publications Series, DESIDOC, Delhi, 2012.

4

Outer Space and International Affairs

Space Security and International Relations: An Introduction

Since the onset of the space age in 1957 with the launch of the Soviet satellite 'Sputnik', thousands of space flights have been launched by several space-faring countries such as the United States (US) and the erstwhile Union of Soviet Socialist Republics (USSR) (now Russia). Almost all space exploration initiatives and space technology developments have been motivated primarily by national security considerations and supported by military space objectives. Outer space, which is generally considered to be above an altitude of 100 km, is unique in the sense that it has no sovereignty rights and hence all of outer space is universally accepted as common to all nations. The Outer Space Treaty (OST) of 1967 signed by over 97 nations,[1] has so far successfully maintained a peaceful balance in outer space, free of any major conflict so that scientific and commercial use of outer space has remained unaffected. While outer space continues to be recognised as one of the domains of 'Global Commons' for peaceful exploitation, several applications for communication, surveillance, reconnaissance, navigation and even use of the Global Positioning System (GPS) for precision weapon guidance have been accepted as legitimate use for national security purposes.

There is thus a distinct and important relevance of space technology for individual nations, in terms of possible use of outer space to serve national security interests. Advances in space technology have now led to the outer space being increasingly integrated with security doctrines of powerful nations, and this has a significant international dimension in terms of security

perceptions of other space-faring nations, as well as the global peace and stability situation. Increasing use of outer space for political-military purposes by a growing number of countries is a cause of serious international concern, because future earth wars and conflicts could invariably spill into the space dimension, for gaining vital techno-military superiority. Technological advances are creating newer space-based capabilities for Ballistic Missile Defence (BMD) and anti-satellite (ASAT) applications are causing certain added concerns of possible military escalation in space that could lead to use of weapons in outer space.

There has been a steady increase in integration of ICT (Information-Communication-Technology) systems with space capabilities for basic modern life-style requirements and for essential international commercial and financial activities. All space-faring nations have thus become critically dependent on space assets for routine as well as critical activities. Therefore, the security of outer space assets as well as competition for space-technology superiority, have become major national security priorities for all progressive nations. However, maintaining peace balance in outer space will require active international cooperation supported by prudent international laws and norms. Ensuring sustainability of outer space for legitimate peaceful exploitation will also require sustained international cooperation. Outer space thus represents a new set of major challenges for the future generation of security strategists, diplomats and foreign policy experts, particularly for space-faring nations and others using space technology.

Today, there are over 50 space-faring nations and the number is likely to increase significantly in future. Each such nation will get increasingly dependent on space-based capabilities—both for civilian and military applications. As technological sophistication offers newer, better and more cost-effective solutions, nations will compete even in the civilian domain for economic gains. As a result, vulnerability of such nations in outer space will get enhanced significantly, with emerging capabilities of international cyber-war, using space assets in the loop. The demonstrated ASAT capability of some advanced nations is already a major space security concern. Further, technology advances such as the Airborne Laser (ABL) of the US, using Directed Energy Weapons (DEWs) and the recent success of X-37B robotic space plane in the US, represent quantum leaps in space capabilities that will certainly accentuate the security perceptions of other nations, as well as influence the world balance of power equations in future. (Some techno-diplomatic details are discussed later in this chapter).

In terms of preserving the sustainability of outer space for vital day-to-day operations, all nations are willingly cooperating for maintaining peace balance in outer space. The International Space Station (ISS) is indeed a shining example of such cooperation. Yet, in terms of techno-military superiority, several space-capable nations may get into serious competition to gain superiority over political or military adversaries. This will thus usher in a new era of cooperation and competition co-existing in the domain of outer space, among powerful nations. This will pose a new range of challenging international situations that future generations of diplomats will have to handle with a sense of techno-security acumen that is not yet very mature. Nations will also re-calibrate security and foreign policy priorities to give due prominence to this new domain of international affairs.

The dual-use nature of advanced technologies and increasing diffusion of these technologies to more nations/users is also of major concern in terms of possible misuse by irresponsible nations or entities. This international dilemma is very much like that of nuclear proliferation control, where the line between peaceful legitimate use and wrongful military use is very thin, but the impact is vastly different. Thus, space technology controls in future may require a different international approach for setting-up robust space laws and ensuring strict compliance by all stakeholders.

Introduction of weapons in outer space by any one powerful nation can tip the delicate international balance and endanger the very stability of space activities for commercial and scientific purposes. The situation is further complicated by increasing problems of space debris created by decades of use of preferred low-earth orbits (LEOs) by thousands of satellites and space flights. Any space accident is a potential disaster as it can cascade into multiple collisions. Hence, there is a concern that emerging rivalry between the US, China and Russia may compromise the status-quo in outer space. The OST and various other existing international agreements have no provisions for preventing possible weapons in outer space and thus, they are not empowered to deal with future space conflict scenarios in outer space. While increasing military competition in space seems inevitable in future, the role of international laws and astute diplomacy by leading space-faring nations will be vital for maintaining global peace and stability.

Being one of the leading space-faring nations, India must comprehensively address its own priorities in outer space and formulate suitable space policy guidelines to protect its national security interests in outer space. Having concentrated mainly on social benefits from its space programmes, India must

now re-calibrate its space policy in recognition of the new realities in outer space, and evolve a space security strategy for itself. Simultaneously, India must also engage proactively, towards building international convergence for preserving peace and stability in outer space.

This chapter presents a brief overview of space technology development and its impact on political-military strategies for future conflict situations, because this will be one of the most important challenges for the future of international relations (I.R.). An analysis is attempted to offer a nuanced understanding of complex inter-connected issues for evolving possible techno-political solutions, to preserve the sustainability of outer space for non-military exploitation. The discussion brings out the urgent need for international consensus on how best to monitor and regulate use of outer space for military purposes, and how to prevent misuse of space technology by rogue elements that might challenge international convergence of interest in outer space. The endeavour will of course be to highlight the Indian perspective and discuss how India may prepare for the future.

Space Security: International Dimension and Indian Perspective

Advances in space technologies over the past few decades have facilitated extensive use of outer space for scientific, commercial and military-oriented applications, and outer space is now indisputably acknowledged as the new critical dimension of modern warfare strategies, as well as national security calculus. Although, the OST was formulated to preserve outer space for peaceful activities, it did not prohibit deployment of space systems for military purposes, as long as no Weapons of Mass Destruction (WMD) were involved. Therefore, although the use of outer space for military support functions such as surveillance, intelligence and weapon guidance may not be classified strictly as peaceful applications, they are nevertheless, not considered illegal because there is no international treaty prohibiting such military oriented applications. As a result, the latest in Revolution in Military Affairs (RMA) is based on network-centric strategies and integration of ICT with satellite systems as a key component. This indicates increasing dependence on outer space capabilities for the national security of individual nations. The role of outer space in defence and security affairs is thus increasing rapidly and its impact on I.R. in terms of balance of power has emerged as the new dimension of international dialogue on global security and stability.

While outer space continues to be accepted as one of the 'global commons' beyond the limited perceptions of national sovereignty of any individual

nation, security of outer space is assuming very large importance for all nations, particularly space-faring nations with their own satellites orbiting space for a variety of applications. Presently, about 50 countries have their own satellites as space assets and the operational security and reliability of these assets have come to assume very high importance for each of these nations because they constitute a vital part of the national infrastructure—both for security as well as economic development. Space is now intimately involved with modern human life-style and most future human aspirations.

As candidly documented in a RAND Report,[2] almost all space explorations have been motivated by long-term political or military objectives. Hence, investments made by powerful nations in developing space technology capabilities are quite substantial, comparable only to investments for defence and security technologies. As is common to most advanced technology systems, the feeder technologies for space capability are dual-use in nature and hence they can contribute to diverse applications of both civil or defence purpose. This creates an interesting situation where rocket technology developed for space exploration can very easily contribute to long-range missile system capability that has very different lethal potentials. Supremacy and control of space technology is already a high strategic priority for powerful nations such as the US, Russia and China. Preventing unfair use of outer space, such as deploying weapons in space is already a very contentious subject among space-faring nations that are the main stakeholders in preserving balance and peace in outer space.

Diffusion of dual-use space technology to multiple users and nations is also of concern, in terms of possible misuse by nation-states or non-state entities. This will be a major new challenge that national security planners and experts in international affairs will have to address in future. Among space-faring nations, space power of adversarial nations can pose threats to national security, but dangers to the sustainability of outer space are already a global concern as they affect almost all nations using space technology for development and progress.

Given the vast scientific, commercial and military potential of space technology and space assets, several countries are striving to build indigenous space capabilities for civilian, defence and security applications. Besides the US and Russia with established leading space capabilities, the European Union (EU) and China are also gaining maturity in space technology, with specific focus on strategic capabilities to meet security concerns. India is also recognised as a major space-faring nation with established indigenous capabilities in all

aspects of space technology. Historically, India's focus has been mainly on civilian application for societal and economic development, with very little attention to leverage space capabilities for security or strategic planning purposes. In recognition of the vital role of space capabilities, both for internal and external security, there appears to be a genuine need for India, to address the security implications of outer space through a suitable policy formulation that is pragmatic and capable of addressing India's vulnerabilities in space. India needs to leverage space technologies to best serve India's national security interests. A well thought-out space policy statement also will serve the purpose of projecting India's strength in outer space.

Space is a high priority for national security in today's world, where most nations are heavily dependent on space assets for almost all important activities concerning development, progress and security. However, building or acquiring military space capability has its own cost and consequences. Before deciding to acquire or pronouncing to forgo space defence capabilities or applicable weapons or technologies, it is necessary to fully comprehend what such weapons and technologies can do and what could be the cost and consequences of acquiring them, as well as the price of not acquiring them. Clearly such policy decisions will depend on individual national perspective; and how far to articulate national policies for international consumption would be a national decision. However, the need for building indigenous capabilities and evolving suitable strategies cannot be disputed. The discussion thus must also address how India may react to adversarial countries acquiring counter-space capabilities and how India can best protect its national security interests in international forums on space related issues.

In India, defence and space activities have been traditionally kept separate and the two departments function pretty much independently. Occasional use of existing civil assets for India's needs to address security concerns may have served a limited purpose so far. But this must change, with space becoming an important dimension of defence and security. Strategic planning for the future will need to include dedicated space capabilities to meet defence and security requirements. Evolution of a comprehensive Space Defence or Space Control policy will require a high degree of integration of space and defence capabilities. While it may be prudent to keep the civilian space agencies free of military inter-connections, rapid development of defensive space capabilities through planned integration of defence research and development (R&D) and a few key private industries in the country, has now become imperative. India must take an independent position on space security

commensurate with its own assessment of its national security priorities in outer space, only when it establishes an overt counter-space capability.

It is thus imperative to develop a comprehensive understanding of the limits of the presently accepted military exploitation of outer space and what may constitute weaponisation of outer space and their security implications for India. In a sense, weaponisation of outer space has already begun, with extensive use of outer space for military functions in tactical warfare doctrines and the recent demonstrations of Ballistic Missile Defence (BMD) technology for ASAT applications. Space applicable weapon technologies were developed in the 1980s but never deployed due to concerns of arms race in space. However, the priorities of powerful nations are changing and the successful tests of the United States Air Force's (USAF's) Airborne Laser (ABL)[3] in 2010 signals the arrival of technology capability for introduction of DEWs in outer space.

Development and deployment of micro-satellites may represent yet another chapter in weaponisation as they are potentially dual-use systems. Satellites weighing less than 100 kg are relatively very easy to launch and also cost-effective. While technology of miniaturisation has enabled these to be very effective for specific applications, this aspect also makes them very suitable for defence roles. Thus, the technology is already well established and its application for space weapon orientation will depend on the intention and motivation of the user nation. While the US today has a declared doctrine of Space Dominance[4] to maintain its supremacy in outer space, priorities for other major space-faring nations such as China and Russia are woven around ways to counter possible US deployment of space-applicable weapons and other space control capabilities for global force projections.

Once any nation goes beyond a certain threshold in defensive-offensive space capability, an arms race in space will be inevitable. Any policy formulation on Space Security by India must take cognisance of the advances in missile defence technology in India's region of influence, and the possibility of hostile forces using outer space against Indian national interests. Though technology options are costly, it is also necessary to understand the cost of not deciding or investing timely, in the context of others acquiring such capabilities and also in the context of imminent technology controls that will become increasingly restrictive for space technologies. Ambivalence may thus prove extremely expensive.

Space Technology Advances

While surveillance by U-2 type spy planes was considered hostile in the 1960s, far superior military reconnaissance capabilities of satellites for military applications are accepted by most nations today. This transition has not been very smooth. The initial thrust of R&D was on improving launch vehicle efficiency and making satellite pay-loads more compact, reliable and robust. The LEOs were of special interest as these satellites provided immediate benefits to expanding surveillance and communication capabilities. Access to higher geo-synchronous orbits became possible with further advances in satellite sub-systems as well as cryogenic technology for lifting heavy payloads to 36,000 km altitude for world-wide communication and for establishing GPS with a multitude of innovative applications. In fact, space technology is often seen as instrumental to the explosion of ICT in terms of instant world-wide connectivity and the new era of information superiority, in the emerging knowledge-based society.

In the race for techno-military superiority during the cold war, ASAT capabilities were created by both superpowers with significant technology spin-off benefits from the R&D efforts for anti-ballistic missile (ABM) systems. The Defense Advanced Research Projects Agency (DARPA) was instrumental in promoting major space technology advances and a significant technological advance was the US announcement of the Kinetic Kill concept in the early 1980s for a new generation of ASAT weapons in which a two-stage missile called the Air-Launched Miniature Vehicle (ALMV)[5] could be launched from a high-altitude F-15 aircraft, to ascend directly to target satellites in LEOs to physically collide with the satellites, thus greatly reducing the time to destruction. The 1983 announcement of the Strategic Defense Initiative (SDI) for BMD again stirred-up a lot of action-reaction technology development activity between the two superpowers and R&D for potential space-applicable weapon technology has continued to date.

While SDI provided the boost for space technologies, the weapon system focus came from the BMD system requirements that invariably used the outer space. Long range missiles (5000 km or more) can attain maximum velocity of about 7-8 km per second (kmps) and if launched vertically, could reach 6000 km altitude to track and target any LEO satellite. Intermediate range missiles (5000 km or less) and short-range missiles (1000 km or less) have slower terminal velocity in the range of 3-5 kmps, may have limited reach into space, but may still have ASAT application against lower orbital satellites. The ASAT capabilities of modern missile defence systems with long range

anti-missile missiles, thus can be very significant and have serious implications for space security perceptions of other nations.

Other known BMD components of US systems include Space Tracking and Surveillance System (STSS), Space-Based Infrared System (SBIR) in low or high orbits, Sea based Radars (e.g. The Aegis), Terminal High Altitude Area Defense (THAAD)[6] for Ground-Based Midcourse Defence and ABL for boost-phase kill of Intercontinental Ballistic Missiles (ICBMs). The US withdrawal from the ABM Treaty in June 2002 cleared the way for development, testing, deployment and even transfer of any or all forms of BMD systems deemed desirable. As such, today there are no international treaty restrictions to testing of non-WMD type weapons in the context of space security.

As already discussed, another promising advance in space technology is that of micro-satellites using micro-electro-mechanical-systems (MEMS) and nanotechnology. These can be deployed by a mother satellite and controlled from the ground, to attach to a target satellite to cause disruption or destruction in suicide mode on command. The US R&D efforts are fairly advanced as demonstrated by the XSS-10 satellite (28 lbs weight) that was tested successfully in 2003. China is also believed to have developed experimental micro-satellites of 30-40 kg weight class, that included solar panels, batteries, computers, charge-coupled device (CCD) cameras, propulsion and telemetry support. A very attractive feature of micro-satellites is that they can be launched at 1 percent of conventional cost, and can be deployed as part of the space defence system. There are no laws or international norms for this new class of satellites which themselves can be potential space weapons. Arriving at universally acceptable agreements on these futuristic issues will pose major challenges to the new cadre of diplomats and foreign policy experts.

The current thrust for space weapon technology in the US can be understood in the context of the vulnerability of its vital space assets. The US Space Command Vision 2020[7] recognises that 'weapons in space' is a matter of time and comprehensive space control must be achieved not only to protect one's own space assets but also to deny the use of space to the adversary, at least in times of conflict. The US Space Command's strategic master plan therefore calls for 'Full Spectrum Dominance' in space by 2020 through integration of space capabilities with information security and defence strategies. The present US response to space vulnerability is largely military,

thus suggesting a kind of inevitability of space based weapons, both for missile defence as well as for protecting satellites.

The US reluctance to support any new proposed treaty such as the one on Prevention of an Arms Race in Outer Space (PAROS) is based on its assessment that at present only the US is capable of deploying space-based weapons and can retain its dominance of space through development and deployment of a new class of weapons for space defence and space control. The US plans reportedly include even the use of possible low-yield nuclear weapons for missile defence and space dominance, in the event where the existing kinetic kill systems fail to achieve the purpose.[8]

While the space technology pursuits of the US provide indicative trends, various other nation-states have also been investing in space technologies for quite some years. The investments are indeed based on national goals, budgetary provisions and availability of technological expertise. Significant developments are taking place in various areas of non-military use of space technologies which are useful in exploring distant planets, human exploration of space, and earth, and space science experiments, remote sensing, weather forecasts and space transportation technologies. Progress by a few advanced countries in military use of space technologies is also very impressive and these serve as catalysts for the evolving RMA as well as for enhancing civilian application horizons.

Space Technology in India

India is one of the few nations in the world with indigenous satellite launch capabilities, as well as the technologies for development of modern high-tech satellites. For historical reasons, much of the Indian expertise and experience has been in the civilian domain, although almost all space technologies are of dual-use nature and can thus be prime candidates for defence and security objectives. India also has its own missile defence programme and significant R&D capabilities in energy beam technologies, that are very well suited for space defence applications. With the role of space technology rising in matters of security and defence, it is natural that these technologies will be closely guarded by those who have it. For example, in the nuclear or missile technology field, developing indigenous competence in such critical technologies will be vital to India's security interests in outer space.

A quick look at Indian Space Research Organisation's (ISRO's) evolution and achievements shows a very promising indigenous capability and expertise that could easily be oriented to serve national security priorities at short notice

if required. However, space and defence activities in India have been kept under two distinct departments through a conscious policy of not inviting defence related technology embargoes for Indian space programmes. This international posture was to keep the opportunities for international cooperation unhindered by strategic considerations as far as possible. The two separate, independent streams approach has not only enabled ISRO to develop critical dual-use technologies useful in outer space without causing much apprehension among neighbouring countries, but also helped India to create an impressive strength in both defence and space sectors, through a natural process of sharing the national knowledge-base and human expertise.

ISRO was established on August 15, 1969 and the Department of Space was set up in 1972. Starting with the launch of the first Indian satellite Aryabhata on April 19, 1975, ISRO quickly developed the indigenous satellite launch vehicle (SLV) by early 1980s and launched the Indian National Satellite (INSAT) series for communication and educational purposes. By early 1990s ISRO developed Indian Remote Sensing (IRS) satellites for earth observation capability and started with the Polar Satellite Launch Vehicle (PSLV) to launch Indian satellites. By the turn of the century ISRO successfully launched even foreign country payloads. By then, the marketing arm of ISRO, Antrix Corporation Ltd. was established to promote international space commerce and cooperation. The year 2001 marked the successful test of the Geosynchronous Satellite Launch Vehicle (GSLV) and the increasing participation of ISRO in international space activities. A good account of ISRO programmes can be found in a book from the Institute for Defence Studies and Analyses (IDSA), New Delhi, co-edited by Dr. Arvind Gupta, Dr. Ajey Lele and the author.[9]

The first two IRS spacecraft, IRS-1A (March 1988) and IRS-1B (August1991) were launched by Russian Vostok boosters from the Baikonur Cosmodrome. The two identical IRS spacecraft hosted a trio of Linear Imaging Self-Scanning (LISS) remote sensing instruments working in multiple spectral bands. The Spacecraft Control Centre at Bangalore oversees all spacecraft operations and spacecraft data transmissions are effected via X-band and S-band antennas at the base of the spacecraft. ISRO and its commercial marketing arm, Antrix Corporation Ltd., successfully launched the much improved IRS-1D earth imaging satellite, weighing 1350 kg in September 1997. These satellites have established capabilities that can be compared to the best in the world.

The IRS-2 series (OCEANSAT-2/CLIMATSAT-1) is designed to cater to global observations of climate, ocean and atmosphere with the help of a Microwave Radiometer and Thermal Infrared Radiometer for observing oceanographic parameters like winds, sea surface temperature, waves, bathometry and internal waves. The National Remote Sensing Centre (NRSC) of ISRO is a key player in the Earth Observation Programme and Disaster Management Support Programme.

The IRS satellites today are the mainstay of the National Natural Resources Management System (NNRMS), for which the Department of Space (DOS) is the nodal agency. Data from the IRS satellites is received and disseminated by several countries all over the world. With the advent of high-resolution satellite imaging, new applications in the areas of urban development, and infrastructure planning, as well as other large-scale applications for mapping have been initiated. Remote sensing applications in the country now cover diverse fields such as crop acreage and yield estimation, drought warning and assessment, flood control and damage assessment, land use/land cover information, agro-climatic planning, wasteland management, water resources management, under-ground water exploration, fisheries development and prediction of snow-melt run-off etc. These capabilities become very important at times of natural disasters or other national emergency situations.

As one of the major space-faring nations in the world today, India has established end-to-end indigenous capabilities in satellite design and development, as well as indigenous launch capability, and infrastructure for all types of orbits and several types of payloads, including launch of multiple payloads using its own command and control infrastructure. India presently has eleven INSAT satellites operating as communication applications and seven IRS satellites. These provide information of value about earth resources and are primarily used to support services towards enhancing public good. The series of satellite assets of India, along with the ground support systems, and other relevant infrastructure represent a national asset worth over $ 25 billion. This is a major asset for a country like India, and security of these assets is clearly a high priority for the nation.

The Indian GPS Aided Geo Augmented Navigation (GAGAN) system is essentially for civil aviation applications in communication, navigation and surveillance. The IRS satellite system is the largest constellation of remote sensing satellites for civilian use in operation today, in the world. All the satellites are placed in polar sun-synchronous orbits and can provide data in

a variety of spatial, spectral and temporal resolutions to enable several programmes to be undertaken, relevant to national development. ISRO's Radar Imaging Satellites (RISATs) carry synthetic aperture payloads that can provide multi-spectral and fine resolution images well suited for security applications as and when required. Similarly, the Indian Regional Navigation Satellite System (IRNSS) is an independent regional navigation satellite system being developed by India, to provide accurate position information service in the region extending up to 1500 km range. This is also a useful asset for national security, if and when required. While India has made impressive progress in the civilian space arena, with its own series of INSAT satellites and other imaging and remote sensing satellites, it has yet to develop an independent military satellite programme.

Cartosat-2 launched by PSLV-C7 in January 2007, is an advanced remote sensing satellite carrying a panchromatic camera, capable of providing scene-specific spot imageries for cartographic and other applications. India is acutely aware of the dangers of high-resolution satellite images falling into wrong hands, and this was voiced by the then President Dr. A. P. J. Abdul Kalam in November 2007 at the IDSA International Space Security Conference. He suggested enactment of suitable laws to govern the use of outer space and regulate the use of data acquired from remote sensing satellites, particularly of sensitive installations. Space laws have to evolve in India to match the sensitivity associated with space imaging capabilities and space security perceptions. Some guidelines for national laws matching world standards are urgently needed to safeguard national security interests.

As India emerges as a potential regional power and an important international player in outer space, it is being closely watched by other nations. The year 2008 saw ISRO successfully demonstrate ability for simultaneous launch of 10 different satellites (2 Indian + 8 foreign) in different orbits. It is interesting to note that in terms of technology, this has major implications for building BMD capability to launch Multiple Independent Re-entry Vehicles (MIRVs).

India's own Chandrayaan-I project of 2008, for exploration of lunar terrain and mineral compositions, was the first ambitious moon-mission by ISRO. Budgeted at Rs. 380 crores ($ 88 million), it will perhaps be the cheapest ever lunar mission. ISRO's agreement with National Aeronautics and Space Administration (NASA) to carry two scientific payloads on board Chadrayaan-1 was seen as a major recognition of Indian space capability. By 2010, future plans of ISRO included indigenous development of cryogenic engine

technology for fully indigenous GSLV flights, manned space missions, further lunar exploration, Mars exploration and interplanetary probes. ISRO has significant field installations and ground assets and cooperates with the international community as a part of several bilateral and multilateral agreements. On November 5, 2013, ISRO launched its Mars Orbital Mission and the Indian mission is currently en-route to Mars. On January 5, 2014, ISRO's GSLV-D5 successfully launched GSAT-14 into the intended orbit. This also marked the first successful flight using an indigenous cryogenic engine, making India the sixth country in the world to have this technology.

On June 30, 2014, ISRO's PSLV III simultaneously launched five satellites of foreign nations into different earth observation orbits and marked a major trend among nations to recognise the maturity of Indian space technology and its reliability for commercial launch of their satellites.

Thus, despite a few failures, which is not very uncommon in space endeavours ISRO has not only established world-class technology capabilities, but has also positioned India as a respectable international partner in affairs of outer space. Given the strategic and security imperatives and the growing trends for use of space for security objectives, India must take informed decisions about investing in space from an exclusive defence and security perspective.

For a country with established capabilities in civilian space technologies and independent space assets, it is imperative for India to remain actively engaged in international negotiations on the subject of security of outer space. Within the country, there is urgent need for an informed debate on the subject, involving policy makers, technology experts, user services and think-tanks. The first priority would be to concentrate on international cooperation to protect existing space assets and enhance indigenous capabilities to remain competitive in space technology and space services domains. Simultaneously, development of critical technologies such as missile defence, advanced sensors, micro-satellites and DEWs must be pursued with renewed focus. This must be aimed at quickly bridging the technology gap with advanced nations, so that India does not again become one of the targets for space arms control.

India's policy of keeping defence and space activities separate and independent must change now, with space becoming an important dimension of defence and security. Strategic long-term planning must now envisage integrating space capabilities with defence capabilities, as may be desired for safeguarding national security interests. Evolution of a comprehensive Space Defence and Space Control policy will require a high degree of integration

and coherence between space and defence departments. An early integration of key private industries in the country will be essential to maintain a high pace of work needed to remain competitive in outer space. Only then, can India take independent positions on Space Defence and Space Control, commensurate with its own assessment of its national security priorities in outer space.

It is very likely that by 2020, security of outer space will become a subject as important as nuclear deterrence is today, because military space capabilities and a new class of energy weapons will directly affect the nuclear-missile deterrence value. Space will then become an even more important new dimension, in the calculations for military and economic power worldwide. If well thought-out policy guidelines are not evolved now, India may by default become a reactive party in international discourse, and a follower of other powerful nations, instead of taking independent proactive steps to best suit its national security interests in outer space.

Space Sustainability, Space Laws and Space Code of Conduct

Sustainability of human operations in outer space is under threat due to orbital space debris. Such debris in LEO ranging in size from 1 to 10 cm in diameter, poses a significant problem for space vehicles and earth observation satellites. While this debris can be detected, it cannot be tracked with sufficient reliability, to orient spacecraft to avoid collision with these objects. Such debris can cause catastrophic damage even to a shielded spacecraft. Orbital debris is not the only form of space junk that is deleterious to earth satellites. Since collisions with asteroids have caused major havoc to the earth's biosphere on several occasions in the geological past, possibility of other impacts in future are quite likely. Such events, together with man-made space debris, are a cause for serious concern for the sustainability of outer space activities, on which modern society has become very dependent.[10]

Functional satellites represent only a small fraction of the estimated 150,000 or more objects which are larger than one centimetre in diameter that presently exist in LEOs. Most of these objects are fragments of larger objects that have broken up during explosions and other events. Since the closing velocities of these objects are roughly 7-8 km/sec, a collision with any one of these objects is likely to cause catastrophic damage to a satellite or space vehicle, such as the Space Shuttle and International Space Stations (ISS).

As the number of pieces of debris in orbit continues to rise, so does the

likelihood of collision. Manoeuvres for avoiding tracked debris have been undertaken by the Space Shuttle and are planned for the International Space Station as well. Furthermore, procedures for dealing with damage are being developed in the event of a collision with orbital debris. Given the technological advances associated with lasers and optics, a ground-based pulsed laser can ablate or vaporise the surface of orbital debris, thereby producing enough cumulative thrust to cause debris to re-enter the atmosphere and burn-out in small pieces, without causing much damage on ground. This is a cost effective method and is attracting a lot of international attention.

The increasing use of outer space has produced a considerable amount of space debris and this has become a major threat to spacecraft and satellites. Growing awareness of the problem of debris has motivated most space-faring States to develop national space debris mitigation standards and in 2001, the United Nations (UN) Committee on the Peaceful Uses of Outer Space (COPUOS) mandated the Inter-Agency Space Debris Coordination Committee to develop international debris mitigation guidelines. In 2005, the Scientific and Technical Subcommittee of COPUOS evolved agreements on intentional destruction of any orbital objects to avoid long-lived orbital debris, and the US Federal Communications Commission (FCC) enacted rules for monitoring debris mitigation plans.

In 2005, the US modernised its Michigan Orbital Debris Survey Telescope and Electro-Optical Deep Space Surveillance systems and is currently actively pursuing space-based surveillance systems. The US network uses 31 sensors worldwide, to monitor over 10,000 space debris objects larger than 10 cm in size, and Russia monitors over 5,000 orbital objects, mostly in LEO, with 14 sensors. The EU, Canada, China, France, Germany and Japan are all developing new space surveillance capabilities. China has also established its first Space Target and Debris Observation Lab.[11] While all such sensors will contribute to manage the dangers from debris, their utility for strategic surveillance for military purposes can clearly provide strategic advantage in future, particularly as military use of space keeps increasing. India has an active interest in international negotiations on debris mitigation and is a constructive participant.

However, the problems of space debris persist. In January 2007, China used a modified ballistic missile with an interceptor on-board, to destroy its own inoperable Fengyun-1C weather satellite. The destruction created more than 3,000 pieces of trackable space debris, which quickly spread across a large region of the earth orbit, covering between 300 and 2,000 km in altitude.

NASA's debris experts estimate that the test created perhaps as much as 150,000 pieces of debris, too small to track. Most of these will remain in orbit, posing a serious threat to working satellites in LEO for decades. On February 10, 2009 an active American iridium commercial communications satellite and an inactive Russian military communications satellite collided accidentally, at an altitude of 800 km. The collision created more than 2,000 pieces of trackable debris that spread along and around the former satellites' orbits and now threaten other satellites in the LEO region. While there was data beforehand showing that this collision was likely, neither the US nor Russia was actively checking these particular satellites for possible collisions at the time.[12]

The US military maintains the world's most extensive orbital tracking network that recorded some 22,000 objects in space, measuring 10 cm or larger as of 2012. What cannot be reliably tracked yet are the objects smaller than 10 cm, because these are too small to follow consistently. Scientists estimate that about 500,000 bits of junk measuring 1 to 10 cm are orbiting our earth, and believe that many millions smaller than 1 cm exist. All objects in the earth's orbit travel at very high speed; therefore even small debris can cripple or destroy working spacecraft or endanger astronauts.

Space sustainability has become a serious issue in the recent past because of its huge implication for the future of mankind. In just about two decades, modern everyday life has become intrinsically dependent on space-based technologies and the vulnerabilities are very serious. This is thus a global concern that must demand global level cooperation for lasting solutions for mitigating space debris and maintaining outer space, particularly the preferred orbits, free and safe for all contributing satellites and space flights. Some kind of control and monitoring will be necessary to ensure this objective for decades in future. This would cause serious challenges to the international negotiators who would be making an attempt to reach global consensus, while protecting national interests in space. Space has thus emerged as an important new dimension for global peace and stability, and diplomats will need to be well informed about technological and legal nuances in this new arena of global discourse.

Besides the threat of debris, space sustainability can also be seriously disturbed by sudden spurt in military activity in space; in response to unforeseen events in the backdrop of absence of clear and accepted space laws or norms.

Some of the 'what if' scenarios may include:

- A military satellite of Nation A on intelligence gathering mission is jammed or destroyed by Nation B in space. What can be the response of Nation A?
- A satellite of Nation A is made dysfunctional by debris hit. Who can Nation A blame or claim compensation from, and under what laws?
- If a dysfunctional satellite of Nation A collides with a vital functional satellite of Nation B. How does Nation A handle international condemnation or claims of Nation B for compensation?
- A ground-based space facility of Nation A is damaged by State-sponsored terrorists. How does Nation A respond to loss of space capability?
- The introduction of a military satellite by Nation A is objected to by Nation B on grounds of disturbing regional stability. What can the international community do to resolve the dispute, to prevent further escalation that can endanger space sustainability?
- If a nation links the PAROS and the Fissile Missile Cut-off Treaty (FMCT) discussions at the Conference on Disarmament (CD) to block possible consensus for formalising space laws or the space code of conduct, what punitive actions can be there against such nations?

Such scenarios can indeed suddenly upset space balance and hence, there is an urgent need to evolve space laws acceptable to all nations. This will be a huge challenge for diplomats negotiating international space treaties or conventions in the future.

Space Laws: Emerging Trends

The increasing exploitation of outer space to serve military and security objectives has brought international space security under serious pressure. Outer space has become a critical tool for achieving foreign policy goals, serving as a force multiplier in war, as well as for strengthening homeland security at all times. Modern defence doctrines are getting increasingly integrated with space capabilities and space assets. Space capabilities also open up hitherto restricted access to outer space for commercial opportunities, such as exploiting untapped resources of the moon, Mars or other celestial bodies. This has created a competitive environment in space, wherein countries are actively aspiring to dominate space beyond terrestrial challenges, and the world leader in space, the US, has a declared policy of continued space dominance.

The emerging global scenario for outer space undoubtedly requires that all space-faring nations including India would have to adopt a proactive approach, both in the context of leveraging outer space for national security, and also for building its ability to compete in the global space market, on the foundation of a balanced and robust indigenous space industry and commerce. India in particular, needs to face up to this new reality of the increasing relevance of space to national security, and calibrate its foreign policy according to the new set of priorities in outer space. (For a detailed discussion of space laws see endnote no. 9).

Outer space is presently being governed by quite a few international treaties and agreements, mainly the OST of 1967. However, the growth of space technologies and their increased use for military purposes have raised serious questions about the possible use of weapons in outer space as a natural extension of the trend of increasing militarisation. It is in this context that the OST needs to be strengthened with additional conventions such as the PAROS, to contain the momentum towards increasing military exploitation of outer space. At the June 2008 meet of the COPUOS, discussions were focused around evolving a potential 'rules of the road' agreement for space activities of the future to support the EU call to consider a more specific code of conduct for space activities. Meanwhile, there are also proposals that COPUOS be given a specific mandate to address long-term sustainability of all space activities.

The consequences of the emerging global space order will have a major impact on India's space security and hence, the subject deserves very careful consideration. International negotiations to arrive at a comprehensive agreement to preserve outer space for uninterrupted peaceful activities, will be one of the major challenges for diplomats around the world, and Indian diplomats and foreign policy experts need to be well informed on all related aspects of space security—political, technical and legal—to protect India's national interests in outer space.

Although there is international consensus that outer space is meant to be used only for peaceful purposes, the term 'peaceful purposes' has never been clearly defined, and it is generally accepted that this would include scientific, commercial and developmental uses as well as support to operational military functions. However, the limits to military use of space are not yet defined in any international treaty. There is thus a need for clearer articulation of the international laws for preventing further militarisation of outer space. India, like other space-faring nations, must evolve its own national laws to safeguard

its national interests, while also allowing for integration with international treaties, norms and conventions.

At present, the emerging space order does not envisage an all-out 'Star War' in space. But for India, the main concerns should include: (a) the deployment of space technologies as a terrestrial force multiplier against India; (b) the possibility of denial of access to outer space through degradation/ destruction of India's space capability; (c) the use or threat of use of space capabilities by unfriendly powers, to pursue their foreign policy objectives against India; and (d) the use of space-enabled technologies for conducting subversive activities and acts of terrorism, including cyber terrorism against India. The challenges are urgent because space events can happen without any warning. India must therefore maintain a constant vigil in outer space using its established capabilities, and leverage its strength in outer space for clear enunciation of its priorities, through careful articulation of its space policy.

Existing international space laws or treaties, formulated under the aegis of the UN to govern all human activities in outer space include the : (a) OST of 1967 (b) Rescue Agreement of 1968, (c) Liability Convention of 1972, (d) Registration Convention of 1974 and (e) Moon Agreement of 1979. India has adhered to the OST, the Rescue Agreement, the Liability Convention and the Registration Convention, but is a signatory only to the Moon Agreement. India's posture in international forums in the context of legislating appropriate national space laws should not only fulfil certain international obligations, but more importantly, it should give India the maximum ability to leverage outer space for national advantage and security.

The OST vide Article III establishes the application of the UN Charter, and the rules of customary international law, to space activities. Furthermore, the prevalent view is that Article 2(4) (*All members shall refrain in their international relations from the threat or use of force against the territorial integrity*) applies to outer space, thus, making it unlawful for a State to interfere in a hostile manner with the space-borne assets of another State. Consequently, a pre-emptive attack based on presumption of threat would be illegal. However, should hostile action occur against a State, it would be legitimate for it to exercise its right of self-defence under provisions of Article 51 (*Right of self-defence).* Thus, given that an armed attack could be carried out either by using space-based assets or by the use of space as a force multiplier, it could be argued that all actions and developments undertaken by a country, to put itself in a state of constant preparedness to ensure national security, and defend and repel a hostile attack from or in outer space, is in consonance with the

UN Charter and rules of international law. This makes developing military space technology capability legitimate, under the present legal framework. The point of law laid down by the UN Charter pertains to the prohibition of its first use. Military response by a country must only be an act of self-defence for it to be legitimate.

The 1967 Outer Space Treaty (OST)[13] represents the primary basis for legal order in outer space founded on the principle of 'peaceful use'. However, the present state of heightened threat perception of a significantly militarised outer space can be seen as a direct consequence of textual ambiguities inherent in the OST. For example, the absence of a 'definitions' clause, gave rise to opposing interpretation by the US and the erstwhile USSR of the phrase 'peaceful use' of outer space. The situation is also exacerbated by the absence of verification and enforcement provisions in the OST. While the US maintains that peaceful use means 'non-aggressive', the USSR insisted that it should mean 'wholly non-military'. That the US interpretation has been more acceptable is obvious from the current international status and practical aspects of space security. Thus, although the international community generally supports measures to prevent an arms race in space and denounces its weaponisation at the domestic level, space powers are unlikely to accept any curbs on their national activities in outer space.

This is also demonstrated in the apparent failure of the CD to prevent an arms race in outer space, bringing it on the verge of weaponisation. Lack of consensus in the UN COPUOS has also effectively prevented further developments in space law since the 1979 Moon Agreement, which remains the least ratified agreement of the five treaties. In the present context, therefore, the moot question is whether space-applicable technological strength deployed as a force multiplier in war, qualifies as 'non aggressive' and 'peaceful use' of outer space.

The CD, Geneva continues to be the most important multilateral forum where efforts are underway to prevent an arms race in outer space. As is well known, the US vote against the PAROS Resolution in 2005, consequent to its unilateral withdrawal in 2002 from the 1972 ABM Treaty, has paralysed the CD. Subsequently, in 2008, Russia and China jointly submitted a draft proposal for a 'Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects' (PPWT), which has also met with resistance from the US and Israel. India needs to proactively analyse the strategic and tactical merits and demerits of supporting the PPWT in the geopolitical context.

Anti-satellite weapons and space debris are the two most serious threats to the security of outer space. Weapons programmes also threaten stability in outer space, as demonstrated by the Chinese ASAT experiment on January 11, 2007 and the US intercept of a failed satellite, using its missile defence system on February 20, 2008. China's ASAT experiment was perhaps the worst debris-creating event in the history of the space age.[14] In light of the above, India should formulate a clear policy and posture about proliferation of anti-satellite weapons systems in the context of Article IV of the OST. Under this Article, the contracting parties 'undertake not to place in orbit around the earth, any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.' It also stipulates that the 'moon and other celestial bodies' are to be used 'exclusively for peaceful purposes' with even conventional military installations, weapons testing and manoeuvres expressly prohibited. But there are no laws to enforce these conditions on defaulting nations.

Another reason for the accelerated race to control outer space is the civilian application of space technology and its subsequent commercialisation since the 1970s. The lucrative returns from the commercial space launch industry, satellite telecommunications, broadcasting and earth observation applications, among others, has made orbital slots and radio frequency spectrum the most coveted natural resources in outer space, particularly as these are limited resources. The International Telecommunication Union (ITU) is responsible for allotting orbital slots and allocating radio frequency spectrum to member-states on a first-come-first-serve basis. As could be expected, powerful space powers including the US, Russia, and the EU dominate the ITU, and tend to control benefits from natural resources in outer space.

Thus, they also have strong motivation to deny other countries access to space. India needs to be watchful and proactive in the ITU to ensure adequate orbital slots and spectrum for itself, and to offset attempts by countries to have the capacity to cause harmful interference with India's activities in space.

In conclusion, an overview of the existing international space law regimes, activities permitted thereunder as against constraints imposed by the treaties, is imperative to enable India to identify realistic goals, strategies, timelines and the posture to adopt, both in the international and national domain, to protect national priorities. There is urgent need for clarity on the question of development of national space doctrines and policies, and an ongoing study

of other space powers that could likely impact India's ability to ensure its own national defence and security.

It is also important to undertake a cost-benefit analysis of the probable negative consequences arising from the absence of an appropriate national space doctrine, space policy and domestic legal regime, to facilitate the achievement of identified goals. Today, national security compulsions provide the foundation for the development of valid national objectives that define space security in the context of its importance to defence, commercial, economic and developmental objectives. In the context of the emerging RMA and the trend for network-centric warfare doctrines that depend heavily on space capabilities, it is obvious that the salience of space technology in India's military modernisation is bound to increase. In the final analysis, it must be recognised that time is of essence because other nations are racing ahead.

Unfortunately, the OST does not expressly prohibit the development, testing and deployment of non-WMD weapons in outer space, nor does it prohibit the development, testing, and deployment of ground-based systems that can reach targets in space, using conventional, nuclear or directed-energy kill mechanisms. As a result, Article IV (of the OST) is often cited to support the claim that all military activities in outer space are permissible, unless specifically prohibited by another treaty or customary international law. By that measure, the Chinese ASAT test in January 2007, or the firing of the SM-3 missile by the US Navy at a dying satellite, or even the deployment of the space component of the US missile defense system does not represent a violation of the OST. It is well known that any de-fragmentation of orbiting satellites or spacecraft will create additional debris and that debris will tend to remain in space for a length of time, depending on the altitude of the event. The higher the altitude, the longer it will take the debris to lose height, to ultimately enter the earth's atmosphere in small fragments, often too small to cause much concern.

In terms of the march of technology towards possible weaponisation of space, two recent developments deserve special mention. One is the well-known US success with testing of the ABL that can target a ballistic missile in boost phase, well above the atmosphere, by using a power laser beam weapon from aboard an aircraft platform flying at about 10 km altitude. The ABL system beam director has adequate look-up capability to target enemy missiles at slant range of about 600 km. It is obvious that such a system situated well above the dense atmospheric layer, can be used easily to destroy LEO satellites that are much softer and predictable targets, compared to a

fast moving missile with a much tougher body. So, while the DEW system can legitimately be deployed for BMD purposes, it would be available to a host country for ready ASAT application, without any preparation time. The ABL project is on hold due to very high cost implications and its own vulnerability to enemy missile or aircraft attack, but the Advanced Concept Technology Demonstration (ACTD) has successfully established the capability, should the need arise in future.[15]

The second potential space weapon, much more cost-effective than the ABL, is the lesser known success of the space plane X-37B developed by Boeing under the aegis of the US Air Force. Also called the Orbital Test Vehicle (OTV), the first OTV launched on December 8, 2010, was the first unmanned spacecraft to return to earth in perfect condition for re-use. The second X-37B spacecraft launched in June 2011 with an Atlas 5 rocket, stayed in orbit for over one year and performed many classified successful tests under NASA's Commercial Orbital Transportation Services (COTS) programme. The space plane is a free-flying, reusable spacecraft with fully autonomous rendezvous and docking capability with the 'International Space Station'. The spacecraft with 6000 kg payload capacity can directly rise to LEOs for multiple missions as well as independent re-entry burn down and water landing capability. Potential for X-37B type spacecraft is enormous in future both for civil, commercial and military missions.[16] These new emerging technological strides actually represent quantum leaps in technology towards possible future weaponisation of outer space.

It is in this context that most progressive nations are engaged in discussions on how best to evolve internationally accepted laws or norms that can preserve space as 'global common' to be shared peacefully by all nations of the world. Since national and global priorities are bound to have different perspectives, strictly binding laws may not work well in outer space; the international community is for evolving a Code of Conduct (COC) in space.

Space Code of Conduct: Diplomatic Challenges

It is well known that ASAT weapons were successfully developed and tested in the 1980s by both the superpowers during the peak of the Cold War but these were not actually deployed then, to prevent a space weapon race between the two superpowers of the time. Since there were only two parties in the game, it was possible to reach an informal agreement in the context of the doctrine of Mutually Assured Destruction (MAD). But now there are multiple players in outer space. However, the US has significantly enhanced its

superiority in outer space to support its declared doctrine of Space Dominance—that emerged from the former US Secretary of Defense Donald Rumsfeld's report on space security and missile defence. The continued enhancement of BMD capability by multiple countries today has created uncertainty about the future of space security. As the genie of technology cannot be put back in the bottle, it is necessary to find ways to prevent adventurism with advanced space technology by any player, because that can easily upset the delicate balance of power in outer space.

Satellites are essentially slow moving soft targets compared to fast moving surface hardened missiles that can be targeted from ground today. Satellites therefore can be tracked very easily from the ground, and hence most satellites are inherently vulnerable to various kinds of attack from ground, aerospace or from outer space. This provides a very simple rationale for developing space applicable weapons to defend satellites. However, for a range of practical and technical reasons, space-based weapons cannot be relied upon to protect satellites. Instead, the primary mission of space weapons is offensive, for targeting the satellites of adversaries and this capability is assumed to provide the deterrence required for protecting national satellites. What started as building space capability to leverage outer space for national security has now become a threat to others and this strategic value of military satellites makes them easy targets of the adversary.

Fortunately, while space has long been militarised — hosting communications, surveillance and navigation satellites to support military operations, it is not yet weaponised by any space-faring nation as a matter of policy, even though there are no international laws or agreements to prohibit weapon in space as long as it does not involve WMD. The US was the first to use space-based GPS technology for precision guided munitions (PGMs) in the Iraq war and since that was not challenged by any country; such a weapon targeting application is now considered legitimate.

So, what constitutes space weapons? Any ASAT system (whether land, sea, or aerospace-based) capable of damaging a satellite or a spacecraft, or interfering with its functioning while in earth orbit, would certainly be classified as a space weapon. Terrestrial weapons that can interfere or damage the satellite's ground stations or ground-based communications receivers are typically not considered ASAT weapons as per present norms. But any weapon on a space-platform that can engage any target on ground, aerospace or outer space could also be classified as a space weapon.

Since there are no official definitions there are indeed some grey areas. For instance, if a platform in aerospace, below 100 km altitude is used to target a missile in ballistic trajectory before it re-enters earth atmosphere, would that be weaponisation of outer space? Probably not, or else anti-missile missiles would be termed as space weapons since they would operate outside the earth's atmosphere. Similarly, if a micro-satellite in space orbit without any explosives collides and destroys another satellite of the adversary, either by accident or in a suicide mode, would that be weaponisation of space? Probably yes, but then what laws would govern such eventualities and how would one fix accountability and liability? If a large piece of debris hits and damages a satellite or space-craft, would that be interpreted as aggression if the countries involved are in a conflict situation? Who would make the rules and get universal agreement on the laws? These are questions with no easy answers.

In 2008, the US announced its proposal to fund a 'Space Test Bed' that could place prototype Space-Based Interceptors (SBIs) and other weapons in orbit. While small numbers of SBIs would not provide a missile defence capability, if properly designed they could readily attack satellites. In addition to being able to attack satellites in low orbits, the large amount of fuel onboard SBIs could allow them to reach satellites even in geosynchronous orbit in roughly one hour. Therefore, other countries would see even small numbers of such weapons as a significant ASAT threat.

As already discussed, powerful lasers from aerospace platforms or even from ground have the capability to disable LEO satellites without actually breaking them up, thereby preventing debris. Such systems may indeed emerge as preferred weapons in space in future. However, there are no laws or norms to either prevent or fix responsibility for such weaponisation. It is for this reason that there is serious international dialogue to formulate an International Code of Conduct for Outer Space (ICOCOS) that can prevent any unwanted adventure in space by any country or group and thus help preserve the sustainability of outer space for the benefit of all.

Besides the concern of use of weapons that can suddenly upset the delicate balance of peaceful activities in space, the other major concern is the problem of increasing debris in space that can cause a series of collisions or accidents leading to more debris and compromising legitimate civilian activities. Space laws and codes need to address both these aspects. The rule-making process undergoes several different stages. These include politico-diplomatic, technical and legal steps that must be debated and a consensus reached, both within and between countries. Only then the rules can take shape as legitimate,

enforceable and accepted norms. Many countries in the West have focused on the technological and safety aspects of outer space. But any universally acceptable rule-making must address the importance of politico-diplomatic endorsement from all space-faring nations, especially the new and emerging space powers.

In 2008, the EU released its Space Code of Conduct (SCOC) which was revised in October 2010. It sought to codify best practices in space activities with emphasis on Transparency and Confidence-Building Measures (TCBMs). The code would be a voluntary mechanism open to all States and is complementary to the existing framework regulating outer space. It preserves the inherent rights of States for collective self-defence in accordance with the UN Charter and States that become party to the code would be bound by the existing legal arrangements. Signatories to the SCOC would need to formulate and implement national policies and procedures to minimise the possibility of accidents in space, collisions between space objects or any form of harmful interference with other States' assets. Participating States would be expected to share information on national space policies and strategies, including basic objectives for security and defence related activities and seek solutions based on an equitable balance of interests.

Some of the ICOCOS proposals are very idealistic but difficult to implement. Most nations are unlikely to openly share information related to national space strategies in the atmosphere of growing competition and geopolitical rivalry, particularly among the more powerful nations—the US, China and Russia. Even though there is general consensus for having an international mechanism for preserving peace in outer space, the EU proposals have encountered many objections from major space powers as well as from new space-faring nations, mainly because formulation of EU SCOC has not been a wider participative process. While the US has not openly opposed the EU draft, a major Washington think tank, the Stimson Center has prepared an alternative draft ICOCOS that also seeks to protect US supremacy in space.[17]

Unfortunately, the history of global arms control measures and technology management agreements shows that more powerful nations often flout international norms when it comes to furthering their own national security or economic agenda. This has been amply clear in the case of the Hague Code of Conduct (HCOC) evolved to prevent missile proliferation which has not managed to achieve any spectacular success. Hence, there is considerable discussion between major space-faring nations to arrive at a set of 'rules of

the road' for space activities and these could then create a set of guidelines for others to follow. Efforts to prevent weapons in space, such as the PAROS Treaty jointly tabled by Russia and China at the CD in 2002 found support from 163 nations but was rejected by the US and Israel. Similarly the China-Russia PPWT proposal in February 2008 was again rejected by US at the CD. This is ample evidence of the challenge that the global diplomatic community will face in arriving at universally agreeable ICOCOS.

For India, the debate must begin with understanding the kind of space future it wants to see in the context of its Asian neighbours and preventing space activities that may be counter-productive to achieving that future. Given that the majority of space debris was created during the Cold War by the large number of military satellites of the US, Russia and Europe, countries to which these assets belonged are unlikely to allow foreign governments or other international bodies to examine or destroy such objects for fear of compromising national security. One can foresee political difficulties emerging over the kind of technology and hardware that would be used to destroy space junk and debris. Destruction of dysfunctional satellites will also lead to problems with States not being able to reach consensus on the procedures to be used. It is not difficult to envisage a scenario where the absence of a consultative process would further complicate the situation.

Satellites play a crucial role in civil, scientific, economic, and military endeavours. With the world's largest investment in space assets, the US has a tremendous amount to lose from deploying space weapons. Legitimising attacks on satellites is short-sighted since other countries will also be able to develop effective ASAT weapons, ultimately increasing the vulnerability of US satellites. Developing weapons can also undermine relations and increase tensions with other countries, which could reduce cooperation needed for progress on issues such as terrorism and thus reduce stability during a crisis. Lastly, if ASAT weapons get to the stage of being used, debris from destroyed satellites can damage other satellites, triggering a chain of collisions to create more debris and thereby compromise the use of space for important civil as well as military purposes far into the future.

An approach to protecting satellites could be smart planning to ensure that any attack or damage to individual satellites would not affect key military or critical civil capabilities. This can be achieved by developing certain redundancy by rapidly bypassing damaged satellites and creating back-up systems in space and ground for uninterrupted functioning. Distributing a single satellite's workload among clusters of satellites can make it more difficult

for an adversary to mount a useful ASAT attack. Such measures have an additional advantage that they negate the attacking adversary any advantage from space adventurism. Better space surveillance, individually or jointly, can also enhance the ability to keep satellites safe from natural and man-created accidental threats by enabling satellites to manoeuvre out of the way of danger.

An ideal SCOC should work towards a universal taboo against attacking satellites or space-craft. It should incentivise cancellation of provocative space weapons development programmes and discourage building new offensive capacities by emerging new space-faring nations. Such a SCOC will require establishment of appropriate Space Laws, rules of the road and transparency measures for space, including consequences for any country that attacks or damages satellites. Space-faring countries have the greatest technical ability to threaten satellites, but they are also the countries with the greatest incentive to develop guidelines that can safeguard the existing peace balance in outer space. It would be imperative for all space-faring nations to come together for a productive international dialogue to quickly and efficiently formulate a SCOC before a chance event or accident further complicates the atmosphere for a wider consultative process to arrive at a global solution. These represent very important future challenges for international foreign policy experts and diplomats or interlocutors, who can conduct informed and constructive discussions for achieving common goals in space.

Policy Options for India and Foreign Policy Challenges

Space is a high priority for national security in today's world where most nations are heavily dependent on space assets for almost all important activities concerning development, progress and security. Before deciding to acquire or pronouncing to forgo space applicable weapons or technologies, it is necessary for any nation to fully comprehend what such weapons and technologies can do and what could be the cost and consequences of acquiring them. It is also imperative to understand the price of not acquiring or developing such capabilities indigenously. While there may be different perspectives to debate how far a nation can articulate its national space policies for international consumption, the need for clarity in building indigenous capabilities and evolving suitable security and economic strategies in space, cannot be overstated.

For India, the internal policy discussion must also address how India may react to adversarial countries acquiring counter-space capabilities and how India can best protect its national security interests in international forums

on space related issues. This calls for a foresighted space policy that integrates national security plans with defence and foreign policies. In India, as already discussed, defence and space activities have been traditionally kept separate and the two departments function pretty much independently. Using existing civilian space assets for occasional needs to address national security concerns may have served the purpose so far, but this must change quickly with space becoming an important dimension of defence and security. Strategic planning for the future will need to include dedicated space capabilities to meet defence and security requirements. Evolution of a comprehensive Space Defence or Space Control policy will require a high degree of integration of space and defence capabilities. While it may be prudent to keep the civilian space agencies free of military interference, rapid development of defensive counter-space capabilities through planned integration of defence R&D and key private industries in the country will be extremely important. Only then India can take an independent position on space security matters commensurate with its own assessment of its national security priorities in outer space. It is thus imperative to develop a comprehensive understanding of Weaponisation of Outer Space and Space Based Weapons and their security implications for India. Technological advances already exist for extensive militarisation of outer space and extensive use of outer space for complex military functions in tactical warfare scenarios. The recent successful demonstration of BMD technology for ASAT application clearly establishes the potential of BMD for space warfare purposes. It is important to note that the priorities of powerful nations in outer space are now changing.

Development and deployment of micro-satellites will represent yet another chapter in possible weaponisation as they are potentially dual-use systems. Clearly the technology is already well established for obvious advantages in civilian and commercial applications and many nations including India are very active in this emerging field. However, its application for space weapon orientation will depend on the intention and motivation of the user nation or group. While the US' focus today is on maintaining its supremacy in space, priorities for other major space-faring nations such as China and Russia are woven around ways to counter possible US deployment of space applicable weapons and other space control capabilities for global force projections. China's growing military strength in outer space is thus justified as a counter to deal with US dominance in space, but for India this poses a problem because the same strength can be used against Indian interests, particularly in the event of any terrestrial conflict with China or its evergreen ally Pakistan. India's space capabilities thus cannot afford to fall behind China.

The above makes it clear that a techno-military race in outer space is already building and once any nation goes beyond a certain threshold in defensive-offensive space capability, a sudden escalation can lead to use of weapons in space. Any policy formulation on Space Security by India must take cognisance of the advances in missile defence technology, DEW capabilities and micro-satellite activities in India's region of influence. Building and enhancing space situational awareness will become very critical and timely sensing of hostile intentions of adversarial nations or groups will be critical to Indian national interests. The technology options in outer space are indeed expensive but it is also necessary to understand the cost of not deciding or not investing timely. The price of inaction may rise exponentially if the technology gap with other leading countries is allowed to widen because then India may end-up facing imminent technology controls that will become increasingly restrictive for future space technologies. Ambivalence may thus prove very expensive for India. US objections to Russian willingness to sell cryogenic engine technology to India, is a case in point.

As a country with world-class capabilities in civilian space technologies and independent space assets, it is imperative for India to be proactive with regard to its own space security perceptions and policies. This would entail remaining actively engaged in international negotiations on the subject of security of outer space while building comprehensive understanding and capabilities within the country. There is thus urgent need for an informed debate on the subject involving policy makers, technology experts, user services and think tanks. The first priority should be to concentrate on international cooperation to protect existing space assets in a cooperative security model and simultaneously enhance indigenous capabilities to remain competitive in the space technology and space services domains. Development of critical technologies such as advanced sensors, missile defence, micro-satellites and directed energy technologies must be pursued with renewed urgency to build indigenous strength. This must be aimed at quickly bridging technology gaps with advanced nations so that India does not once again become one of the targets for possible space arms control regimes in future.

It is very likely that by 2020 outer space capabilities will become as important as nuclear deterrence has been for the past five-six decades because strategic space capabilities will directly affect the nuclear-missile deterrence value. The 1972 US-Soviet ABM Treaty was a clear acknowledgement of the impact of outer space capability on BMD effectiveness. After the collapse of the Soviet Union, the US was quick to abrogate the 1972 Treaty obligations

so as to proceed with missile defence plans in space. Space is thus acquiring an ever-more important dimension in the calculations for techno-military superiority. If proactive policy guidelines are not evolved timely, India may by default, become a reactive party and a follower of other nations with limited choices. This is the rationale for a need to address all aspects of space security in the Indian context and for the need to evolve practical and effective policy guidelines for India's response to the emerging threat of increasing militarisation of outer space.

In view of the fast growth of the Indian economy and the future needs of national security, India must articulate a space policy to announce its unambiguous intentions to utilise space capabilities for the purpose of addressing national security concerns. Such a policy, which would *inter alia*, indeed reiterate India's commitment to the use of outer space for peaceful purposes, must also articulate how India may use space capabilities for the purposes of national security. This is a legitimate use of space, and for this, India will have to undertake strategic long-term planning aimed at integrating specific space capabilities with defence capabilities for safeguarding national security interests. India will also have to constantly monitor the development of space and missile defence capabilities of other space powers including those of China (and as a consequence, Pakistan), and be acutely aware of the possibility of hostile forces using outer space against Indian national interests.

India must remain actively engaged in international discussions and negotiations on issues concerning the use of outer space for civilian and military purposes so that it could be in a position to shape and influence international negotiations on space-related issues to best serve its national security interests. India is already globally participative in efforts to mitigate space debris problems. Simultaneously, it would be imperative for India to develop a comprehensive understanding of concepts like 'weaponisation of outer space' and 'space based weapons', so that it can evolve a suitable response to an arms race in space, particularly in the context of safeguarding India's national security interests in outer space.

India's space assets are critical to its economic and human development goals. Space capabilities are also critical for national security and regional balance of power. India needs to evolve and articulate a National Space Security Policy to formulate and implement space security strategies commensurate with the perspectives of the defence services and national security interests. Space policy should help enact legislations of appropriate national space laws to meet international obligations and also protect national interests. This

should provide guidelines on how India may respond to any hostility in space. India must urgently invest in technologies critical to space security and establish indigenous capability in counter-space technologies and systems. There is urgent need for international consensus on how best to monitor and regulate use of outer space for military purposes within certain limits, to prevent a new arms race in outer space. The international community must also prevent misuse of space technology by rogue elements that might challenge the international convergence of interest in outer space. India, being one of the early starters and a major space-faring nation, must address its own priorities in outer space and formulate suitable strategies to protect its national security interests. In the changing global security scenario, space defence has assumed a very critical dimension.

China's aggressive advances in counter-space capability, arguably in response to the US space policy pronouncement for full-spectrum dominance in space, can pose 'clear and present' danger for India, where increasing dependence on advanced space capabilities will be extremely vital both for economic progress and for national security. Therefore, it is imperative for India to acquire certain minimum counter-space capabilities to protect its national security interests in outer space through its own indigenous technology capabilities. This must indeed be backed with well articulated space policy guidelines and the political-legal institutional framework necessary to enable effective implementation of India's space policy. The declaration of a National Space Policy as demonstration of political will and space defence capabilities are essential to building deterrence in space. While doing so, India must also contribute proactively towards building an international consensus for preserving the 'Peace Balance' in outer space.

NOTES

1. Report of the IDSA-Pugwash Working Group on *Space Security: Need for a Proactive Approach*, Appendix I, "Outer Space Treaty 1967", Academic Foundation, 2009, pp. 79-89. (The author was a contributor of the Working Group).
2. Robert Preston *et. al.*, "Space Weapons Earth Wars", *RAND Project Air Force*, at www.rand.org/publications/MR/MR1209 (Accessed May 14, 2014).
3. "Airborne Laser System (ABL) YALIA, United States of America", at www.airforce-technology.com/projects/abl *(*Accessed May 14, 2014).
4. The US military's doctrine of 'Full spectrum dominance' means control of land, sea, air and space. See https://www.princeton.edu/~achaney/.../Full-spectrum_dominance.html (Accessed May 14, 2014).
5. "Air-Launched Miniature Vehicle (ALMV)", July 21, 2011. It is an Anti-Satellite Weapon. See http://www.globalsecurity.org/space/systems/almv.htm (Accessed May 14, 2014).
6. Two Terminal High Altitude Area Defense (THAAD) interceptors are launched during a

successful intercept missile defence test, September 2013 at www.mda.mil/news/gallery_thaad.html (Accessed May 14, 2014).

7. *US Space Command Vision for 2020* (pdf), December 2005 at www.worldacademy.org/files./The_US_Space_Command_Vision_for_2020.pdf.. (Accessed May 14, 2014).
8. James Clay Moltz, "Increased commercial interests and the evolution of space weapons", *Future of Space Security*, July 1, 2002, at http://www.nti.org/analysis/articles/future-space-security/ (Accessed May 15, 2014).
9. Arvind Gupta, Amitav Mallik and Ajey Lele, (Eds.) *Space Security: Need for Global Convergence*, Pentagon Security International, 2012. Chapter 4—'International Space Laws: Future Outlook' gives a comprehensive discussion of the subject.
10. Brian Weeden, "Economies of space sustainability", *The Space Review,* June 4, 2012 at www.thespacereview.com/article/2093/1. (Accessed May 15, 2014).
11. Inter-Agency Space Debris Coordination Committee (IADC) is an international organisation for ongoing cooperative activities for debris mitigation options. See www.iadc-online.org/ (Accessed May 15, 2014).
12. "Russian and U.S. Satellite Collide", *BBC News*, February 12, 2009, at http://news.bbc.co.uk/2/hi/7885051.stm (Accessed May 15, 2014).
13. Outer Space Treaty, UNOOSA at www.unoosa.org/oosa/SpaceLaw/outerspt.html (Accessed May 15, 2014).
14. "Understanding China's ASAT Test", Union of Concerned Scientists. See http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/us-china-.. (Accessed May 15, 2014).
15. Dwayne A. Day, "Blunt arrows: the limited utility of ASATs", July 6, 2005, at www.thespacereview.com/article/388/2 (Accessed May 15, 2014).
16. Leonard David, "US Air Force's Secretive X-37B Space Plane Shatters Orbital Endurance Record", March 27, 2014 at http://www.space.com/25245-secret-x37b-space-plane- orbital-record.html (Accessed May 15, 2014).
17. Dylan Rebstock, "A Revised and Stronger International Code of Conduct for Space", Stimson Center, Washington DC, November 5, 2013, at www.stimson.org/.../a-revised-and-stronger-international-code-of-conduct... (Accessed May 15, 2014).

5

Cyber Space and International Affairs

Introduction: Cyber Space—The New Dimension

What started as an age of digital electronics and computers in the middle of the 20th century, has gradually transformed modern human society quite comprehensively as a growing population of highly informed people, who are interconnected more via knowledge exchange than commodity exchange. This transformation has been driven mainly by the spread of Information-Communication-Technology (ICT) leading to rapid growth of social and intra-national interactions with its impact on international relations (I.R.) and the political discourse. Politics is often mostly about the evolution of social relationships between nations and people in terms of 'who gets what, when, and how'. It should thus be easy to understand the transformative role of ICT as it has established a new dimension for international exchanges that happened through various forms of physical medium in the past. This new dimension is called cyber space which is creating a paradigm transformation in the scope and speed of human interactions.

The most fascinating development of the Digital Age has been the quick evolution and establishment of an interconnected and standardised network of computers and communication systems across the world as a virtual domain, which is now being recognised as the cyber space. This 'network of networks' has developed into a global system of interactions spanning innumerable shared activities as well as exchange of information and ideas by people around the world through the internet. Activities in cyber space have very quickly acquired

a central role in everyday human activity and indeed in interactions between nations. This is why significant resources are now being invested to address various aspects of cyber space, including cyber security and cyber politics that have the potential to impact global affairs in a major way in the future.

Over the past two decades, cyber technology has demonstrated its promising potential of influencing international relations and even promoting international peace and democratic norms. Cyber space has also proved to be a new dimension of virtual reality that has helped the rise of globalisation and provided new opportunities for global capitalism and commercialism.

While some of the openness and anonymity of cyber space has provided a voice for the oppressed, thus triggering a social transformation and giving empowerment to non-state groups in some autocratic States, the same empowerment of individuals or small groups beyond their limited physical sphere of influence, has the potential to pose serious asymmetric threats to State apparatus for security and governance. Like most other advances in technology, ICT is also double-edged—its impact is based on the intentions of the user. Potential for misuse of cyber space is however enormous, because of its ubiquitous nature and nation-states are waking up to the rise of this new dimension of threat to national security. This maze of interconnected networks—the internet—has caused a revolution with both positive and negative implications and States are now discussing how best to control this new 'animal' to prevent its misuse and yet encourage common good.

It is important to note that the internet was originally designed by the Defense Advanced Research Projects Agency (DARPA) as a medium of fast information exchange for strategic applications. Once its global potential was realised it was decided to allow access to all and hence, the open character of the internet was consciously designed into the system by the creators and built into its architecture. While the internet was designed this way, it can indeed be changed as political actors contest the design of this open architecture and compete to use the new technology to gain superiority over the adversary. This is possible between nations, groups or even individuals, and this duality of technology for cooperation or competition highlights the core of the modern-day relationship between technology, society and politics. As technology spreads and impacts a wide range of actors and the things they value, inevitably some of these actors will contest the architecture of cyber space and seek to redesign it at a technical level, and even exploit it at the application level, in order to advance their specific interests. Some of this has already begun to happen.

The central issue of governance of cyber space, among the variety of international stakeholders—including States, international organisations, non-governmental institutions, private firms and other non-state actors—is about the technical standards, regulations and institutions that determine the structure and applicability of cyber space. It is therefore important to understand how novel models of international governance may be constructed to adjudicate disputes among States and other international stakeholders, such as how the internet ought to be structured, used and regulated. Main concerns are about the role that States may play in this process and how future of I.R. may be affected by such over-reaching technologies that go beyond sovereign borders.

Cyber technology holds major promise for international economic development through rapid spread of what is now recognised as 'knowledge economy', which emphasises the potential gains in economic growth that could be achieved from a greater ability to quickly send, access and store information on a global scale. Cyber space is the new medium for the improved flow of knowledge which itself can be considered as being 'good for economic progress.' Diffusion of information technology (IT) along with international economic liberalisation opens up ways to allow capital to flow across borders and be invested in 'good ideas'.

On the other hand, the diffusion of cyber technology can also create and deepen a 'digital divide' between developed societies that are capable of better harnessing technology for productivity gains, and less developed societies that are not. This increasing gap could ultimately create a security problem as those who feel excluded from the global information society and its wealth creation potential can turn to violence to capture some of the gains.

This brings to focus the relationship between cyber space and international security, which can include a wide variety of phenomena such as cyber crime, cyber conflict, information security, or even cyber warfare. Application potential can range from access to tactical or operational information, and strategic attacks on critical infrastructure, to espionage and propaganda for political or economic objectives. It appears clear that ICT has served as the foundational element of latest revolutionary network-centric operations which enabled the integration of capability-enhancing technologies into modern strategic capacity and superior operating systems. ICT has provided an efficiency-booster or multiplier effect that allows modern militaries to quickly distribute large volumes of information and analyse them in order to identify

what is strategically useful. Such information operations (IO) can disrupt an adversary's information systems and include psychological operations, military deception, electronic warfare and computer network operations (CNO).

In global affairs, power depends upon the context and the rapid growth of cyber space is an important new context in the world of politics. The low cost of entry, relative anonymity and asymmetries in vulnerability allows smaller actors to have more capacity to exercise influence in cyber space than in several more traditional domains of world politics. The cyber domain is both a new and a volatile man-made environment where power of information is manifesting itself in a new and novel manner. In cyber space the power differentials among various actors is reduced and this provides a unique diffusion of power that is becoming typical of global politics in this 21st century. However, diffusion of power does not mean equality of power or replacement of State as the most powerful actor in world politics. Cyber security today is all about how sovereign States can organise to protect national security sensitivity from asymmetric or adversarial players in the field. The most important implications of cyber space as a new domain of interaction is the emergence of some new features of I.R. which are due almost entirely to the construction, growth and expansion of cyber space. Many of these features are already influencing if not challenging traditional theory, policy and practice of I.R.

In the virtual space of cyber space with no boundaries, the emerging Digital Domain is expanding quickly with the establishment of newer interconnected networks of computers and communication systems across the world that affects every aspect of the life of nations or citizens. Today, this 'network of networks' is evolving into a global system of interactions spanning innumerable shared activities and exchange of information or ideas by the people around the world. It is now common to speak of the sum of these inter-connections among computing and communication systems as a single, shared virtual domain—the cyber space and talk about 'Internet of Everything'.

The activities in cyber space have acquired a very central role in everyday human activities and of course in interactions between nations. This has revolutionised the scope and speed of access to information and knowledge, thus providing unprecedented capabilities to an individual or a nation. At the same time, the same ability to interconnect and access information can have dangerous implications if applied with negative intentions by State or

non-state actors. Some of this is already happening among the religious fundamentalist groups and organised crime syndicates.

In the context of international relations there is growing realisation, that controlling misuse of technology is going to be a difficult challenge because intentions or evil designs have become more important than the tools with which such intentions may be practiced. Fortunately, technology does offer various defensive methods such as fire-walls or encryption to prevent hacking or unauthorised access to sensitive information. However, perceptions of cyber security transcend national geographic boundaries and thus, dealing with cyber security at all levels will demand greater cooperation and coordination among peace loving nations.

This chapter will present a techno-political perspective on cyber security and highlight the major impact of this evolving new technology on 'International Affairs' in general and more specifically on challenges for Indian security priorities.

Expanding Cyber Space: Impact on International Affairs

Governance of cyber space is characterised by the contestation among a variety of international stakeholders including States, international organisations (IOs), non-governmental organisations (NGOs), private firms, and other non-state actors—over the technical standards, regulations, and institutional interactions that determine the structure of cyber space. As already mentioned the open architecture of cyber space was consciously designed into the system by the creators of the internet and built into its structure for world-wide applicability. While the internet was designed this way, political actors contest the design of this architecture and demand changes for better control. This duality touches the core of the relationship between technology and politics and highlights the mutually embedded relationship between them. As the technology spreads and impacts a wider range of actors and the things they value, these actors will contest the architecture of cyber space and seek to redesign it at a technical level in order to advance their particular interests.

Hence, cyber space is an area where technology and international relations are intertwined more intrinsically than many other domains of technology in international affairs. To understand the above premise one can look at the phenomenal growth of ICT that has created a Global Civil Society—civilian transnational groups that can exist and function across international borders and operate independently of the authority of States. These groups, networked

through and empowered by cyber space, could together form the basis of a new and transformative global polity or 'public sphere' that could reshape world politics, impact international relations and even promote international peace and democratic norms if properly oriented by global powers.

Cyber space has thus proved to be a new dimension of virtual reality that has helped the rise of globalisation and provided new opportunities for global capitalism and commercialism. The most important implication of cyber space as a new domain of interaction is the emergence of some new features of I.R., those that are due almost entirely to the construction, growth and expansion of cyber space. Many of these features are already influencing if not challenging traditional theory, policy, and practice of I.R.

While considering cyber space in terms of its impact on I.R., it is important to understand some of the layers of cyber space:

The information—in its various forms and manifestations—that is stored, transmitted, and transformed in cyber space.

The people—that is, the users and constituencies of cyber venues, who participate in and shape the cyber-experience—who communicate, work with information, make decisions and carry out plans, and who themselves transform the nature of cyber space by working with its component services and capabilities, and by making direct and indirect demands for the construction of new functionalities.

The logical building blocks that make up the services and support the platform structure of the cyber space.

The physical foundations that support the logical elements as well as the fundamental physicality that enable the 'virtual' manifestations of interactions.

While it is common practice today to associate cyber space with the internet, with its particular approach to interconnection, a bunch of computers in isolation would not constitute what can be described as the cyber space. It is the structure of interconnections and the constant flow of information that makes cyber space. Though the foundation of cyber space is a *physical* layer —the physical devices out of which it is built—yet cyber space is a conceptual space of interconnected computing devices. Its foundations are the personal computers and servers, supercomputers and grids, sensors and transducers, and various parts of networks and communications channels etc. Communications may occur over wires or fibres via radio transmission or by the physical transport of the computing and storage devices from across places.

Physical devices such as routers or data centres exist in a place and thus sit within a jurisdiction.

The physical foundations of cyber space are fundamental logical layers. Cyber space is not a fictional conception without any physical grounding but a real artefact built out of real elements. The nature of cyber space is such that its strengths and limitations derive more from the decisions made at the logical level than the physical level. The internet, for example, provides a set of capabilities that are intentionally separated to a great extent from the details of the technology that underpins it.

The decisions that shape the internet arise at the higher layer—the logical layer where the open platform nature of the internet is defined and created. Within the logical layer of the internet, one can see a series of sub-layers that provide services to the next sub-layer above. Low-level services include programme execution environments, mechanisms for data transport and standards for data formats. The basic transport service of the internet, which moves packets of data from a source to a destination, is an essential element of this lowest sub-layer of the logical layer. Out of these low-level components and services are built applications, such as a word processor, a database or the Web. In turn, by combining these, more complex services emerge. For example, by combining a database with the Web, we get dynamic content generation and active Web objects. On top of the Web, we now see services such as Facebook that are themselves platforms for further application development.

The nature of cyber space involves a continuous and rapid evolution of new capabilities and services, based on the creation and combination of new logical constructs, all running on top of the physical foundations. Cyber space, at the logical level, is thus a series of platforms, on each of which new capabilities are constructed, which in turn become a platform for the next innovation. Cyber space is very plastic, and it can be described as recursive; platforms upon platforms upon platforms. The platforms may differ in detail, but they share the common feature that they are the foundation for the next platform above them.

Above the logical layer we find the information layer. The creation, capture, storage and processing of information and 'content' is central to the nature of cyber space. Information in cyber space takes many forms such as, the music and videos one shares, the stored records of businesses and all of the pages in the World Wide Web. The contents may include online books

and photographs, information about information (meta-data) and information created and retrieved as we search for other information (as is returned by Google). This information layer contains the implied meaning of the information and content that is transmitted, shared, changed, and augmented and the like. The top layer is the users. People are not just passive users of cyber space; they define and shape its character by the ways they choose to use it, in this sense, they are active participants. The people and their character which may vary across regions, is an important part of the character of cyber space. If people contribute to Wikipedia, then Wikipedia exists. If people tweet, then Twitter exists. This is a critically important, definitional, feature of cyber space.

At the information layers, we find a range of actors with diverse capabilities and providing different services. Google delivers a searchable index of the Web. Companies like Netflix, Google and Apple iTunes sell music and video content over the internet. Some applications are centralised from a control perspective but highly distributed technically, for reasons of performance. These include high-volume content sources such as YouTube or Netflix. The providers of Web pages are perhaps the most obvious example of 'information layer actors'—they include commercial sales and marketing sites, free sites supported by advertising, government information and service portals, and so on. All these businesses are based on ingenuity and innovation, buttressed by market creation capability.

Two important points to note are that the protocols and standards of the internet define not just technical interfaces, but interfaces between separate business entities, and secondly, almost all of this vast universe of actors, large and small, are highly dynamic entities of the private sector, many of which exist and function beyond the authority of any single sovereign State. To date, the makers and users of the internet are predominantly in the private sector, following certain principles of private order, not necessarily controlled by the power of the State.

The selection and effective implementation of cyber security technologies requires:

- Ensuring that the technologies are securely configured;
- Considering organisational information technology infrastructure needs when selecting technologies;
- Implementing technologies through a layered, defence-in-depth strategy;

- Utilising results of independent testing when assessing the technologies' capabilities;
- Training the staff on the secure implementation and utilisation of these technologies.

The organisations in government and critical infrastructure sector would have to protect their networks, systems and data through deployment of access control technologies (for perimeter protection, authentication and authorisation), system integrity measures, cryptography mechanisms and configuration management. Indigenous research and development (R&D) is an essential component of national information security measures due to various reasons, a major one being export restrictions on sophisticated IT products by advanced countries. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Success in technological innovation is significantly facilitated by a sound science and technology (S&T) environment and an ecosystem for continuing innovation where the rate of obsolescence is rapid.

Use of software virus to interfere with the adversary's network is emerging as a new age weapon for Distributed Denial of Service (DDoS) attacks. It may find increasing use in future as was evident in 2012 when the US used 'Stuxnet' to target specific industrial control systems in Iran, to slow down nuclear reprocessing activities. Israel is also known to have used a cyber weapon against Syria and in recent years several cyber attacks are suspected to originate from China. Cyber weapon technology can be used for the purpose of espionage or for compromising C^3I (Command, Control, Computers and Intelligence) networks of the enemy. Building defences against cyber attacks or reducing vulnerability of one's own critical networks is a complex and evolving process shrouded in secrecy. Recent exposure about the US National Security Agency listening-in and monitoring the phone conversation of European leaders has brought-out the dangerous aspects of cyber space that may change the baseline for I.R.

Given the natural inclination for computers and software development, India has made an early start in utilising cyber space for development as well as defence. India recently released the National Cyber Security Policy that highlights Indian priorities and the Indian approach to leveraging the technology to best protect national interest.

International Laws and Limitations: For now, international laws cannot answer satisfactorily the questions about the complexities of cyber space. These laws can at best be categorised into two main types. First is *Jus Ad Bellum* meaning Laws of Conflict Management—these laws mainly give guidelines about the situations in which defensive force should be applied. Second is *Jus in Bello* meaning Laws of War—these explain what are the ways in which offensive or defensive force should be applied.

Unlike domestic laws which have limited jurisdiction and are enforced upon citizens of the State, the problem with international laws is that States may agree to follow them or refuse to follow them or even agree first and then back-out. This means, States which are not signatories to treaties or conventions which would bring them under one umbrella, can cause serious impediments to cyber space laws that can be applied universally. Thus, cyber space neither respects geographical boundaries nor jurisdictional laws, and consequently it may not even honour international laws.

Such an ambiguous and complex dilemma has emerged because ICT has ironically evolved from military communication technology where it was meant to be under tight control of government order. But since its very inception, ICT has empowered individuals to use it at his/her free will and do so as per his/her own requirement or knowledge. This has blurred the separating line between the military and civilians. Lack of precise domestic laws and enforcement makes it difficult to regulate when it comes to civilian use. As a result, civilians too can take a stance just as the Russian authorities took no responsibility in the case of Estonia (discussed later in the chapter). Hence, controlling cyber space use and punishing any violation of norms or laws is very difficult. In the year 2010, 1600 cyber crime cases were registered in India but only seven got convicted.[1]

On the other hand, there are big possibilities of false accusations and victimisation while enforcing cyber laws. For example, there was a case in Japan where four people were arrested for a cyber crime they never committed. In reality, their computers were controlled by a Remote Access Trojan (RAT) virus and the real perpetrators remained anonymous. The mistake was later recognised by law enforcement authorities but by that time, the damage was done to the dignity of those innocent people by the media.[2] Cyber space thus opens up a plethora of new complications and there are wide possibilities of its misuse, affecting many cases where responsibility will be difficult to establish and many mistakes might never get corrected. This can pose new

kind of challenge for diplomats managing international affairs in an environment of fuzzy accountability and an unclear legal framework.

Information Technology, Security and Impact on International Affairs

National security is at the core of State interests in cyber space in the Information Age, as it throws up new modes of conflict and influence. Cyber war is different from actual war and definitions can be confusing because they focus more on intentions rather than actual war-like operations. Actions and reactions take place in the invisible domain of cyber space with no immediate human casualty.

Involvement of the State security apparatus leads to militarisation of cyber security, but the exact war fighting domain is often difficult to define. Often, there are differences in perception of possible impacts of cyber security threats and hence, there can be significant differences among States trying to develop a *modus operandi* and relevant strategies in cyber space in order to secure their interests. Military conceptualisation and doctrines for cyber threat response must take into account technological advances in the emerging network-centric environment of today.

Increasing involvement of non-state actors in the security realm however, can increase the chance of politically motivated cyber attacks with an asymmetric impact on I.R. It is often difficult to determine if a cyber attack is from an independent entity or agency outsourced by a government. In the present transitional phase of cyber security, there are many grey areas and until some structures and international norms emerge, there is a lot of scope for misunderstanding between nations, which can adversely affect otherwise smooth international relations. Foreign policy and practice will have to factor-in such issues in the future management of international affairs.

At the national level, vulnerabilities of critical infrastructure can include: (a) Energy (b) Transportation (c) Communication (d) Water and Sanitation (e) Financial and Banking Infrastructure (f) Industrial Processes and (g) Government Administrations. All of these in modern society are based on digital control systems and threats can be directed against the Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control processes in various critical infrastructure facilities by changing or stopping them. Science fiction often shows the way terrorists take over such critical control systems and cause havoc; in a sense, reality may not be far removed from fiction.

Cyber Space Norms

The internet and social networking have introduced new forms of communication which can be de-linked from national boundaries, authorities and official monitoring. This means every individual can be included in cyber space which gives all cyber issues a truly global character. Hence, the requirement for international norms or conventions regarding the use of cyber space has assumed increasing urgency. International negotiations are required to bring out a set of norms acceptable to the most powerful and pragmatic States, so that cyber space is not fragmented due to competition between nation-states.

A set of good norms should ideally satisfy the following requirements:

1. Cyber space should remain open, interoperable and reliable.
2. All nations should have an interest in clean, healthy cyber space and consequent to that interest, they should have a duty to assist, inform and educate one another.
3. Together all nations should strive for a cyber space that retains the trust of its users.
4. Fundamental freedom of people for information and connectivity would need to be upheld.
5. Key international laws, norms, and rules should be extended to cyber space.
6. Multi-stakeholder stewardship involving governments, international organisations and the private sector should shape the development and maintenance of cyber space.
7. Governments should refrain from political interference in technical development and standards for the internet.

The problem with the current approach towards norms is a 'military capability' mindset. There is little experience of cyber attacks in a war-like context and insufficient knowledge of their consequences. In addition, threats cannot be explained in terms of distinction between say, military vs. civilian, attack vs. espionage, State vs. non-state agents, or intentional vs. accidental. The responsibility of States for attacks originating in their territories, perpetrated by non-state actors, will be hard to define and the involvement of military units in protecting domestic critical infrastructure from cyber attacks can pose new complexities. Handing the military a lead role in responding to a cyber attack on infrastructure could bias the conflict process towards retaliation and escalation, rather than resilience and recovery, because it introduces an offensive

option and action. Having said that, there can be situations where retaliatory action is indeed required.

Cyber Security Policy: Case for India

A good cyber security policy must make India's stance clear in its diplomatic relations and it must be credible for suitably influencing international perceptions. This is important now since international laws and conventions regarding cyber space are in the process of being formulated. India needs a central body which would deal with all aspects of cyber space and acknowledgement of the private sector as being a major player in cyber space. The private sector also needs to be fully participative and on the same page as the State on issues of security and national interests.

The release of the Cyber Security Policy (CSP) of India in July 2013 was an important step in recognising the critical impact that cyber space can have on national security. India has been recognised as a provider of world class IT and telecom products and services for over a decade now. The much awaited CSP 2013 is a right step in protecting and furthering strategic objectives of our nation. India's dependence on ICT is bound to increase in the immediate future with greater emphasis on e-governance to improve efficiency and transparency. The intent, ability and motivation of the government and other crucial stakeholders in this effort would be to protect critical information, technologies and infrastructure. The maturity of the policy and quality of people responsible for implementation will be deciding factors in the survivability and success of the cyber space objectives for gaining strategic advantage in cyber space.

The policy includes a formal assessment of what constitutes India's critical infrastructure sector and the designation of critical technology sectors which will be crucial to our nation's security and stability. The policy envisages creation of a nodal agency at the centre to direct all efforts, assign responsibilities and perform advisory functions for all stakeholders concerned. The central agency will monitor the accomplishment of policy goals and uphold the tenets of accountability. The policy envisages an ambitious goal of training nearly 500,000 cyber security professionals in the next five years who will have considerable potential capabilities equivalent to an army of IT warriors. Public-private partnerships (PPP) have been identified as the key to implementing the policy on the ground and the government has openly endorsed and welcomed participation of India's private telecom and IT companies.

But the underlying principles and the balancing of national security versus the privacy laws of citizens have not been clearly articulated in the Indian policy paper and would be a source of friction in the future. The policy should have made references to the IT Act 2000 which is a law that can have precedence over the policy issued by the executive/government of the day in case of variance or conflict. The concept of checks and balances is also not clearly discussed as to how data will be collected, processed, analysed and distributed and for what purpose, in order to safeguard it against misuse by vested interests.

India needs to set up and promote centres of excellence for cyber security and techno-legal research. However, the policy is silent on the requirement to develop cyber offensive capabilities alongside cyber defence and security. The policy should be flexible and dynamic in nature to incorporate the ever-changing environment of cyber space. There is a need to involve not only industries and ministries but also academia, institutes of higher education and research labs to create an enabling cyber ecosystem. The CSP will play a crucial role in defining the state of the nation in the years to come, through its ability to deliver on the policy vision which is 'To build a secure and resilient cyber space for citizens, businesses and government'.

Following are some salient features of India's National Cyber Security Policy:[3]

1. Based on key policy considerations and the threat landscape, the draft policy identifies priority areas for action.
2. Identifies *PPP* as a key component.
3. Identifies key actions to reduce security *threats and vulnerabilities.*
4. Suggests establishment of a *National Cyber Alert System* for early watch and warning, information exchange, responding to national level cyber incidents and facilitating restoration.
5. Defines role of sectoral CERTs (Computer Emergency Response Team) and establishment of local *incident response teams* for each critical sector organisation.
6. Encourages implementation of *best practices* in critical information and government infrastructure protection through creation, establishment and operation of an *Information Security Assurance Framework.*
7. Establishes framework for *crisis management plan* for countering cyber attacks and cyber terrorism.

8. Identifies priorities for action for *legal framework* and *law enforcement capability* development.
9. Defines priorities for *international cooperation* for information sharing.
10. Identifies indigenous *R&D* as an essential component of cyber security and enlists thrust areas for R&D.
11. Identifies major actions and initiatives for *user awareness, education, and training* (capacity building).
12. Defines *responsible actions* for network service providers, large corporate and small/medium and home users, to secure information and systems.
13. Identifies various *stakeholders* (ministries and government departments only) of cyber security and their responsibilities.

There is genuine need for better PPP in India for quick maturity in cyber space. If the Critical Information Infrastructure (CII) which can include various important private sectors like banking, telecom, energy, airlines, water supply etc. does come under cyber attack, adverse effects do not remain limited to the organisation alone, but can affect multiple entities all over the nation. That is why better coordination as well as information sharing among the public/private sector and cyber security providers like Indian Computer Emergency Response Team (CERT-In), NASSCOM (National Association for Software and Services Company), NCSC (National Centre for Science Communication) etc. is very necessary.

This would provide more case studies and help improvise defence mechanisms as well as build the heuristics for better proactive defence. The government must ensure that CII entities follow computer security auditing as per standards and keep themselves up-to-date so that mishaps can be avoided. Also a budgetary allowance is necessary for all the backroom efforts to maintain momentum. This will make the infrastructure more vigilant, disciplined and up-to-date with compliance issues, thus giving a better edge in cyber security. IDSA, Delhi has brought out a task force report on the subject which is very informative.[4]

Research in both encryption implementation and encryption breaking techniques is necessary to help build lawful interception capabilities within Law Enforcement and Intelligence Agencies (LEIA) as in other countries. Indian private sector and academic institutions should also be included and encouraged to conduct such research and training of personnel.

Technology sharing with other countries which have comparable or better capabilities would be useful. For example, Indian telecom networks use only

a 40-bit encryption system. The basic reason being that India currently has the capability to 'break' it. The capacity should be increased for better safety in various services ranging from e-governance to online banking. Cyber security courses should be introduced at school, graduate and postgraduate levels. With better funding and scholarships, indigenous technology and human resources can be developed for this field.

Cyber space technology tends to develop very rapidly. Hence, cyber intelligence officials and information security personnel need to have latest knowledge. They should be encouraged and funded by the government to upgrade themselves regularly by taking courses. At the same time, not only do the indigenous certifications and training programmes need to be at par with well-known leading private sector certification standards, but these need to be started urgently. This could in turn improve indigenous capability and cut training cost dynamically.

The most famous cyber war incident to date and one with most details in the public domain is the Stuxnet worm in 2012. Stuxnet's existence was first reported by security blogger Brian Krebs. It appeared in dozens of countries targeting what are known as programmable logic controllers, which are ubiquitous industrial computers, the size of cigarette cartons. Stuxnet was specifically designed to harm controllers processing uranium fuel at a nuclear facility in Iran. People who have analysed the attack think someone slid a thumb drive with a Stuxnet code into a Windows personal computer that was linked to the centrifuges, which were buried in a bunker. The worm then ordered the machinery to spin too fast, eventually destroying it. While all this happened, Stuxnet remained hidden from the Iranian technicians at the facility. The worm also disabled alarms and fed the workers fake log reports that assured them the centrifuges were operating just fine.

Stuxnet set Iran's nuclear programme back by months. It did not merely compromise some database like most computer worms, but also obliterated something physical. "Stuxnet was the equivalent of a very high-powered ballistic weapon," says Ed Jaehne, the chief strategy officer at KEYW Corporation, a fast-growing computer security firm in Maryland. As researchers dissected the technology and hunted for motives, some of them pointed to the US or Israel as the worm's likeliest place of origin.

Another example is the Edward Snowden controversy exposing the US Government's PRISM programme. The US has not only spent millions of dollars on PRISM but the seriousness of the initiative can be understood by

the fact that the US NSA employs nearly the maximum number of mathematicians in the world, which is an indicator of its potential to collect and make sense of the vast amounts of data in the cyber domain. All these countries have forward looking programmes, not only to protect their own turf but also to exploit the vulnerabilities of others.

Cyber Security: Threat Perceptions and Policy Dimensions

Cyber threats are best described as: 'A potential cause of an incident, that may result in harm to Information and Communication Network systems in cyber space, and can cause further inconvenience, damages or risk to national security.' These threats are peculiar because a cyber attack could be very difficult to trace back to its origin or may be disguised as if originating from a completely different location.

If one reflects on the 2007 Estonia attacks, there were many threads leading one to believe that Russian authorities had something to do with those attacks but Russia called accusations of its involvement 'unfounded', and neither the North Atlantic Treaty Organisation (NATO) nor the European Commission experts were able to find any proof of official Russian Government involvement.[5] This means that even though in some instances, these attacks are traced back to their origin, it is very easy for the accused to deny their involvement and defend themselves against 'false or miscalculated' accusations. The moral of the story: There is a great need for clearer and comprehensive international norms to deal with such conflicts. Fortunately, after years of monitoring and analysing cyber attacks, there are some generalised patterns that can be deducted by information security analysts. These patterns provide some heuristics and help to provide some direction to further investigation. The benefit of such patterns is that even though the suspects/accused can deny the accusation, some defensive strategy can still be thought out and implemented for the future.

Cyber threats can be put into four main categories: cyber warfare, cyber espionage, cyber terrorism and cyber crime. Also, the first two, cyber warfare and cyber espionage tend to give birth to a complex mechanism to resolve cyber conflict. Their scope is larger than that of cyber terrorism and cyber crime and one must examine the very ethics of cyber conflict. Dorothy E. Denning, an American expert on information security and Professor at the Department of Defense Analysis at the Naval Postgraduate School, Monterey, California, deals with ethical issues related to cyber conflicts.[6]

Cyber warfare is more difficult to deal with than conventional warfare because it is a 'non contact war'. It does not involve any physical or kinetic actions on the adversaries. One State may attack another State's information systems not only to disrupt or destroy their operations, but also for espionage and covert actions in the interest of national security. The conventional Law of Armed Conflict (LOAC) cannot be directly applied to cyber warfare due to its virtual and complex nature.

Since information systems work on the borderline of civilian and military characteristics, it poses different questions about warfare and ethics in using the new dimension of this dual-use technology.

- Is it ethical for a State to penetrate or disable the computer systems of an adversary State that has threatened its territorial or political integrity?
- If so, what are the ground rules for such attacks?
- Can cyber soldiers attack critical infrastructure that serves both civilian and military functions?
- If a nation is under cyber assault from another country, under what conditions can it respond in kind or use armed force against the assailant?
- Can it attack computers in a third country whose computer networks have been compromised or exploited to facilitate an assault?

When 'Hacktivism' or 'cyber terrorism is done by non-state actors, the State needs to deal with additional issues such as: (a) Is it ethical for a group of hackers to take down a website that is being used for illegal activities (according to that group); (b) Can the hacktivists protest by defacing websites or conducting web "sit-ins"?[7]; (c) Can they attack vulnerable machines in order to expose security loopholes with the goal of making the internet more secure?

Another aspect about cyber security is attacking for defence, which can further generate new complexities, such as:

- If a system is under cyber attack, can the system administrators counter-attack in order to stop it?
- What if the attack is coming from computers that may themselves be victims of compromise?
- Since many attacks are routed through chains of compromised machines, can a victim "hack back" along the chain in order to determine the source?

Cyber Security: India's Position

The current world economic scenario is transforming in leaps and bounds due to the rise in ICT capabilities but at the same time, risks are also on the rise because of the imminent nature of cyber threats. According to World Bank statistics, by the end of 2013, internet users in India comprised 15.1 percent of the total population.[8] The internet currently contributes $30 billion to India's Gross Domestic Product (GDP) which might rise to $100 billion, up from the present 1.6 to 3.3 percent by 2015. The internet-related economy would influence India more than the education sector and would be as large as the healthcare sector, in terms of share of GDP at present.[9]

So, it becomes very important to secure India's critical information infrastructure (CII) as well as to come up with better laws and norms to handle cyber threats. Various techniques are used to start cyber attacks from simple social engineering to complex computer programmes and high-end technologies. These attacks may be initiated by some smart college going kid tinkering with a computer system just for fun or some terrorist organisation or 'hacktivist' group or, a nation-state with real sophisticated techniques and resources.

Although India's ranking in cyber crime activities has always been fairly high, but it does not convey that India has committed such activities or holds the capability of defending its cyber space either. In fact, a large number of people in India who are frequent users of the internet do not even know the basic requirements for securing computers. The rate of software piracy is also very high in India. According to the 2011 Global Software Piracy Study done by an independent firm, Business Software Alliance (BSA), about 63 percent of Indians used pirated software. Over 20 percent of respondents in India admitted to acquiring software illegally "all of the time", or "most of the time" or "occasionally", while 23 percent said they do it "rarely." This means that in more than six out of ten cases, software that Indian users installed were unlicensed.[10] People tend to install pirated operating systems' versions due to lack of knowledge, disinformation by the vendor or even do so voluntarily to save some money. Such software can make systems open and vulnerable to hackers. This increases the chance of remotely controlled computers forming dense 'botnets' within the country, posing risks to both Indian as well as global cyber space.

In year 2011-12, India stood third after the US and China as origin or 'Geographic Region of Malicious Activities' with a total share of 6.5 percent

in the global average. With 16.2 percent of malicious activity originating in India, more recently the country was ranked in second position. India then had over 150 million internet users, which was the third largest population of internet users in the world then. About 17 percent of spam zombies were located in India, making it the first in that category. The number of internet users has been climbing very steeply in India in recent years. Indian internet users were estimated to be about 243 million in June 2014 and the number may reach 500 million by 2018. These are huge numbers, making India the highest user of cyber space.

Cyber espionage presents a whole different set of issues because the major share of cyber space operations and control is by the private sector. In fact, the development and management of cyber space was started with efforts of major IT companies and civil bodies. To counter the competition or overpower the competition in the market, often espionage strategies are used as a means to the end. This is done worldwide and it is not restricted to cyber space, but the complexities and parameters are different.

According to a report by Verizon, a security consultants group, which incorporated data from 19 global partners—it covered 47,000 reported security incidents and 621 confirmed data breaches in 2012. According to the Data Breach Investigation Report 2013, 92 percent of breaches are perpetrated by outsiders, while 14 percent have an insider connection.[11] Big technology giants too face espionage problems. In an espionage attack in February 2013, Microsoft, Apple, Facebook and Twitter may have compromised accounts of over 250,000 of its customers. But when it comes to cyber space, the high amount of ambiguity due to absence of precise laws and norms, and lack of public-private sector coordination makes the situations worse. Companies may not want to reveal the damage they've suffered due to concerns about possibly scaring off potential or existing customers, damaging their stock value or incurring potential legal liabilities.

Some of the major organisations in India for the State to gain more control include:

1. National Information Board (NIB)
   The NIB is an apex agency with representatives from relevant departments and agencies that form part of the critical minimum information infrastructure in the country. NIB is entrusted with the responsibility of enunciating the national policy on information security and coordination on all aspects of information security

governance in the country. The NIB is headed by the National Security Adviser.

2. National Crisis Management Committee (NCMC)
   The NCMC is an apex body of the Government of India (GoI) for dealing with major crisis incidents that have serious or national ramifications. It also deals with national crises arising out of focused cyber attacks. The NCMC is headed by the Cabinet Secretary and comprises of Secretary level officials of the GoI. When a situation is being handled by the NCMC it will give directions to the Crisis Management Group of the Central Administrative Ministry/ Department as deemed necessary.
3. The National Security Council Secretariat (NSCS)
   The NSCS is the apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the Secretariat to the National Security Council.
4. The Ministry of Home Affairs (MHA)
   The MHA issues security guidelines from time to time to secure physical infrastructure. The respective Central Administrative Ministries/Departments and critical sector organisations are required to implement these guidelines for strengthening security measures in their respective infrastructure facilities. The MHA sensitises the administrative departments and organisations to vulnerabilities and also assists the respective Administrative Ministry/Departments.
5. The Ministry of Defence (MoD)
   The MoD is the nodal agency for responding to cyber security incidents with respect to the defence sector. The Integrated Defence Staff (IDS) of the MoD is the nodal tri-Services agency at the national level to effectively deal with all aspects of information assurance and operations. The MoD has also formed the Defence CERT whose primary function is to coordinate the activities of the Service's and MoD-CERTs. It works in close association with CERT-In to ensure perpetual availability of defence networks.
6. Department of Electronics and Information Technology (DeitY)—
   The DeitY is under the Ministry of Communications and Information Technology, GoI. DeitY strives to make India a leading player globally in IT and at the same time take the benefits of IT to every walk of life for developing an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion and policies in electronics and information technology.

7. The Department of Telecommunications (DoT)
   The DoT under the Ministry of Communications and Information Technology, GoI, is responsible for coordinating with all Internet Service Providers (ISPs) and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In and other government agencies. The DoT provides guidelines regarding roles and responsibilities of Private Service Providers and ensures that these Service Providers are able to track the critical optical fiber networks for uninterrupted availability and have arrangements of alternate routing in case of physical attacks on these networks.
8. National Cyber Response Centre (CERT-In)
   CERT-In monitors Indian cyber space and coordinates alerts and warnings of imminent attacks. CERT is also responsible for detection of malicious attacks among public and private cyber users and organisations in the country. It maintains a 24x7 operations centre and has working relations/collaborations and contacts with CERTs, all over the world; and sectoral CERTs, public, private, academia, ISPs and vendors of IT products in the country. It works with government, public and private sectors and users in the country and monitors cyber incidents on a continuing basis throughout the extent of incident, to analyse and disseminate information and guidelines as necessary. The primary constituency of CERT-In are organisations under the public and private sector domain.
9. National Information Infrastructure Protection Centre (NIIPC)
   NIIPC is a designated agency to protect the CII in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including national defence. It gets prepared threat assessment reports and facilitates sharing of such information and analysis among members of the intelligence, defence and law enforcement agencies with a view to protecting these agencies' ability to collect, analyse and disseminate intelligence. NIIPC interacts with other incident response organisations including CERT-In, enabling such organisations to leverage the intelligence agencies' analytical capabilities for providing advanced information of potential threats.
10. National Disaster Management Authority (NDMA)
    The NDMA is the apex body for disaster management in India and is responsible for creation of an enabling environment for institutional

mechanisms at the state and district levels. NDMA encourages the development of an ethos of prevention, mitigation and preparedness, and strives to promote a national resolve to mitigate the damage and destruction caused by natural and man-made disasters, through sustained and collective efforts of all government agencies, non-governmental organisations and people's participation.

11. The Standardisation, Testing and Quality Certification (STQC) Directorate
    The STQC Directorate is a part of the DeitY and is an internationally recognised Assurance Service providing organisation. The STQC Directorate has established nation-wide infrastructure and developed competence to provide quality assurance and conformity assessment services in the IT sector.
12. Sectoral CERTs
    Sectoral CERTs in various sectors such as Defence, Finance (IDRBT), Railways, Petroleum and Natural Gas, etc., interact and work closely with CERT-In for mitigation of crises affecting their constituency. Sectoral CERTs and CERT-Ins also exchange information on latest threats and measures to be taken to prevent the crisis.[12]

In the face of increasing cyber threats, the armed forces are now finalising the plan for the creation of three new tri-Service Commands to handle space, cyber and special forces, which will be 'critical' in deploying capabilities for conventional as well as asymmetric warfare in a unified manner. Yet, if one observes all the readiness to deal with cyber attacks and compares that to China or the US, India has a long way to go.

So far, India has signed Memoranda of Understanding (MoU) with the US, the United Kingdom (UK), Japan, Germany and France[13] which would help initiate dialogues in various areas.

For instance the one with the UK focuses on:

- Enhancing international cooperation to reduce the risk of threats from cyber space to international security.
- Strengthening bilateral cooperation to tackle cyber crime.
- Further strengthening bilateral operational partnerships to identify and respond to threats from cyber space and raise mutual resilience.
- Collaborating on building skills and capacities to tackle threats from cyber space and to use ICT for the objective of economic and social development.

- Using existing cooperation between universities and business communities to develop synergy in research and development on cyber issues.
- Creating a global multilateral, democratic and transparent system of internet governance with participation of all stakeholders.

These MOU will benefit India in information intelligence sharing and technology cooperation. India is also developing relations with South Korea, Taiwan and Israel for similar cooperation.

Some special features of cyber security can be summarised as:

One: Technological innovations aside, the single most fundamental feature of this new reality is, the *dominance of the private sector* in an international system defined by the principle of sovereignty and shaped by the demands and capabilities of sovereign States. Cyber space governance is defined more by areas of responsibilities and less by traditional principles of accountability.

Two: The major actor that constitutes and defines international relations, the State is not able to control the cyber domain or to insulate it-self from the implications of new cyber realities. Cyber threats to national security include the militarisation of cyber space, threats to critical infrastructure controls and various types of cyber crimes and espionage by adversarial States or entities. Recent Wikileaks episodes showed in unambiguous ways the politicisation and disruptiveness of cyber space.

Three: The increasing evidence of *cyber threats* to security reinforces the politicisation of cyber space and its salience in emergent policy discourses.

Four: New types of *asymmetries*—notably the extent to which weaker actors can influence or even threaten stronger actors (such as press reports of anonymous penetration—incidents of the US government computer systems)—has little precedence in world politics.

Five: The creation of *new actors*—some with formal identities and others without—and their cyber empowerment, is altering the traditional international decision landscape in potentially significant ways.

Six: The growing *contestation of influence and control* over cyber venues between the new institutions established to manage cyberspace (Internet Corporation for Assigned Names and Numbers—ICANN, IETF (Internet Engineering Task Force) and the traditional international institutions, (such as the International Telecommunication Union [ITU] or other United Nations [UN]

organisations, create new tensions of legitimacy and responsibility, which further complicates the already thorny issue of international accountability.

Seven: Various types of *cyber conflicts* (between and within States, of known as well as unknown identity and provenance) are becoming apparent, with the potential for new modes and manifestations thereof. Many of these contaminate the traditional calculus of conflict and cooperation and its assumptions that are anchored in the physical domain, largely derived from the historical experience of major powers. These are based on the assumptions that the military instruments of power dominate, the identity of the contenders are known, and that, in the final analysis, "might" can be relied upon to make "right", and so forth.

Eight: Concurrently, we are also observing different modes of *cyber collaboration* in the effort to reduce uncertainty and introduce some measure of order in an environment that is increasingly perceived as "anarchic". Among the most notable initiatives is the development of CERTs, a loose network of organisations in different parts of the world seeking to take stock of, and reduce, breaches of cyber security.

Nine: There is a new cyber-based mobilisation of *civil society* (the aggregations of individuals in their private capacity as well as organised elements of the private sector) and its potential empowerment across jurisdictions and in all parts of the world.

Ten: The *intersection in spheres of influence*—with the private sector managing order in cyber space and the sovereign authority managing order in the traditional domain worldwide, spheres of influence can be overlapping and a cause for a unique set of problems for management of international affairs relating to cyber space.

Cyber Weapons

The experts define a Cyber Weapon as a computer code that is used or designed to be used with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings. Over the years many cyber weapons have been identified. For example, a virus Stuxnet, (as already discussed) is one of the well-known cyber weapons used that led to the introduction of many different classifications for their qualifications.

Cyber weapons have existed for years mostly with military and national intelligence agencies. Security experts have confirmed that work by Northrop Grumman, Raytheon and General Dynamics, the stalwarts of the traditional

defence industry have been helping the US Government to develop cyber capacity to spy on or disable other countries' computer networks. The industry started to change around 2005, when the Pentagon began placing more emphasis on developing hacking tools, specifically as a means of conducting warfare. The shift in defence policy gave rise to a flood of arms dealers that trade in offensive cyber weapons. Most of these are 'black' companies that camouflage their government funding and work on classified projects. "Five years ago, there was an explosion that occurred and people with offensive cyber capabilities just burst onto the scene." says Kevin G. Coleman, the former chief strategist of Netscape and author of *The Cyber Commander's eHandbook*, a downloadable guide.[14] Two of the primary weapons in a cyber warrior's arsenal are botnets and exploits. A botnet is a collection of tens or even hundreds of thousands of computers that have been commandeered without their owners' knowledge. Hackers spend years building these involuntary armies by infecting peoples' computers with malicious code—self-propagating computer worms—that remain hidden and prime the computer to receive orders. When activated, a botnet can take down networks by bombarding them with digital chatter. It can also help to spy on and, if needed, sabotage large numbers of machines.

An *exploit*, in hackers' parlance is a programme that takes advantage of vulnerabilities in widely used software such as Windows from Microsoft or in the millions of lines of code that control network-servers. The hacker uses an exploit to break-in, and inserts a worm or other destructive payload. Weaknesses of such software are fairly well known, though software vendors can still take months, even years, to create safety patches to plug the holes. The most valuable exploits are those that are unknown to everyone else until the first time they are put to use. These are called zero-day exploits. (The day the attack is discovered would be Day One.) In the hackers' underground, the invite-only online chat boards where illicit wares are sold, a zero-day exploit for a network running on Windows can perhaps sell for up to $250,000. Stuxnet used four high-end zero days, establishing itself as a highly admirable all-star effort in hacker circles.

Very much like the cold war, the 'Code War' does not reward show of force. Cyber weapons fall into the category of 'brittle' technology, susceptible to the swift development of countermeasures. Once you know how a weapon works in cyber space, it can cease to be a weapon. Low visibility profile is another dimension of 'Code War' where traditional military logic can fall apart in the conflict zone. Deterrence and arms treaties are but philosophical or

perceptional concepts when invisible weapons are involved. Assigning certain blame for an attack may be impossible when it's conducted through computers in dozens of countries. The fear of retaliation, which kept the Cold War from becoming hot, may not necessarily apply here.

An interesting classification of cyber weapons is based on spectrum of action and on this scale one can make a distinction between the following categories:

- *Low potential end of the spectrum* is a malware able to affect systems from outside but is not able to penetrate the target or to create direct harm. This category of tools and software is often used to generate traffic to overload a system or service to create a temporary effect without permanent damage. (e.g. Denial of Service attack)
- *Medium potential end of the spectrum* is any malicious intrusion we can identify that is not able to influence the final target but is able to create functional and physical damage. In this category one can include a generic intrusion agent like malware that is able to rapidly spread and disable sections of a system.
- *High potential end of the spectrum* is an agent that is capable of penetrating the target while avoiding any protection built-in, thus creating direct harm to the victim. This could be the case of a sophisticated malware that could harm a specific system like the virus, Stuxnet. Inside this category, one can introduce a further distinction between learning agent and intelligent agent. Stuxnet is an intelligent weapon without learning capabilities, and one can expect that these features will be part of next generation of cyber weapons.

The cost and complexity of cyber threats are related to the category that they belong to, considering also that behind high potential agents there is a long and considerable content of intelligence, used to acquire information on final targets and develop the weapons specific for them.

Why the use of a cyber weapon has proved a winner?

- First, the disclosure of such agents is silenced because of the nature of vulnerabilities that can be exploited. The study of new zero-day vulnerability provides a real advantage to those who attack and the related risks of failure of operations are minimal. The anonymous nature of the offenses, allows one to circumvent the approval by the world community for a military offensive.
- The costs of developing solutions such as this are relatively low

compared to other conventional weapons for comparable cost to the enemy.

- The choice of cyber weapon allows those who use it to remain anonymous until military strategies deem it appropriate. The main strategies for use of such malware could be mainly aimed at:
  - o Probing the technological capabilities of the enemy. The ability of an agent to infect enemy structures is symptomatic of inadequate cyber defence strategy that may suggest additional military options.
  - o Undermining those that are considered critical structures whose operational support and functions are vital for governmental control.
- There is no doubt regarding the efficacy of these weapons. Events have proved that they are offensive weapons designed with the intent to infect the opponent's electronic networks and structures. The cyber weapons can be designed to hit specific targets while minimising the noise related to the usage of the weapon which can result in their discovery.
- The vector of infection can be of various kinds such as a common Universal Serial Bus support, being able to hit a very large number of targets in a small time interval etc.
- Another significant factor is the inability to predict or observe the development of a cyber weapon by intelligence agencies. In a classical context, the development of a conventional weapon can be easily identified through intelligence operations on the ground and via satellite observations. The development of a cyber weapon is rather difficult to locate as even a private home may be suitable for the purpose.

It is pertinent to understand that it is not necessary that a cyber weapon must be for an offensive purpose; as such many projects for the virus development scan can also be intended for defensive purposes, which is an interesting usage of cyber weapon technology, developed to defend one's systems and track back any cyber threats.

Are we ready to face a cyber attack? In recent years international opinion has been strongly sensitised on this issue and hence, there have been significant investments for building safeguards against cyber warfare. Numerous studies have demonstrated the need for very robust cyber security strategy, defensive and offensive. Unfortunately, many critical infrastructures are still vulnerable

to such cyber attacks. It is therefore necessary to monitor the development and proliferation of these types of threats.

However, since a single country cannot build a very high level of cyber attack immunity alone, it calls for robust international collaboration and mutual cooperation; which in turn calls for very sensitive diplomacy, backed up with the knowledge of finer nuances and implications of cyber technology. The key critical infrastructures required all over the world for such an objective must be identified under a common cooperative defence policy. India still has much work to do.

Challenges for Indian Foreign Policy and Diplomacy

India must foresee and plan for various challenges because of the growth of internet and digitalisation of governance. Failure to do so can be catastrophic and could affect national security, the Indian economy and social stability. India is particularly vulnerable to threats from cyber crime, cyber terrorism, cyber espionage and cyber warfare. India's critical infrastructure is also vulnerable. It is only a matter of time before cyber space becomes an independent theatre of war. The US has begun to regard cyber space as the fifth domain of warfare. It has set up a cyber command and come out with a 'Cyber Doctrine' and reserves the right to respond in an appropriate manner if attacked in cyber space. Many countries are responding by setting up similar structures. Several countries are doing R&D on cyber weapons and this raises concerns regarding possible random weaponisation of cyber space.

This chapter aims to underline the urgency of having a cyber security policy and institutional structures to address emerging challenges. Protection of critical infrastructure will require robust policies and sustained public-private partnership as much of the internet infrastructure is owned by the private sector. India will also have to ensure that there is coordination, cooperation and international uniformity in legal measures both among private and public entities. There are two stances that India can opt for now, it can either involve itself in international efforts to construct newer legal frameworks for cyber space, or stay aside till it becomes self-reliant, enough to be heard as a credible voice and play a constructive and important international role with other powerful and influential nations. To determine the correct choice is a dilemma because there are a lot of indeterminate parameters. And time could be running out.

The Budapest Cyber Space Conference held in October 2012 is the only

international platform till date which brought all nation-states together to put forward some norms. As usually happens, there were three major stances by the conferees: Liberal Democratic (the US, the UK, NATO countries), authoritarian States (Russia, China) and countries like India following their legacy of Non-Alignment. When it comes to Cyber Treaties some nations are in favour of adopting a new global treaty and some strongly oppose it. In fact, it might be too early to bind States into any new legal instruments when the future of their activities in cyber space remains uncertain and no one quite knows how to apply existing laws to the current state of cyber domain. Though legal experts are aspiring to bring out some rule book which would provide blanket guidelines for all cyber conflicts, in reality, it is not possible to do so without very vigorous discussion at international platforms.

In this sense, negotiating such a treaty is a cumbersome and time consuming process. Nevertheless, States are still developing their cyber capabilities and formulating strategies. Things tend to change rapidly in cyber space technology and any treaty negotiated now could be obsolete in no time. It might take a decade or so to negotiate a cyber space treaty. For example, the Budapest Conference agenda has been in discussion since 2003 and yet neither has it been fully implemented by member states nor have many States joined it. Consensus has been difficult due to ideological differences.

Hence, it would be advisable to come up with easily amendable and changeable norms. It will not only help in better International Cyber Cooperation among the States but also provide flexibility to change them as per the pace of the technology. CII is mainly controlled and owned by the private sector. More government involvement in their operations might cause hurdles in development and trade. Hence, government partnership with companies, and optimising information sharing and data security is inevitable.

However, if norms are put in the following manner, it would suit India better.[15] States should distinguish between disruptive and damaging cyber attacks and evaluate an attack on the basis of its scope, duration and lethality.

1. States have a duty to assist other States that have suffered a major cyber attack or disaster and also have a duty to inform others of new threats in cyber space.
2. States should cooperate in the certification of ICT supply chains.
3. States whose territories or citizens are involved in trans-border cyber activities which are unambiguously criminal in their States should

cooperate in the investigation of these crimes and the apprehension of their perpetrators.

4. States should enable the formation of public-private partnerships for cyber security, which include both local and international ICT companies operating in their territories.

The above suggested norms are likely to be acceptable to most and are also easier to adapt. They aim to reduce vulnerability and confrontation rather than suppressing threat actors. If all States behave according to these norms, there will be significant reduction in threats and conflicts. Also, these norms focus on maintaining cyber space security for all States instead of fulfilling ambitions of a few. They are the types that are 'status quo' oriented to maintain stability of cyber space.

The internet is seen here in its true form as a Network of Networks which would remain useful only with a growing and contributing number of users. So, it becomes a positive sum or classic cooperative game. However, it becomes difficult as the competition between States for superior status and power grows. Hence, development of indigenous technology and capability for reasonable deterrence becomes a necessity.

The third point mentioned above in relation to norms is specific. As regards the ICT supply chain the focus is on the management of cyber security requirements for IT systems, software and networks. These ICT supply chains could be influenced or subverted in ways that would affect normal, secure and reliable use of IT. Inclusion of malicious hidden functions in IT can undermine confidence in products and services, erode trust in commerce, and affect national security. As disruptive activities using ICT grow more complex and dangerous, it is obvious that no nation may be able to address these threats alone.

Confronting the challenges of the 21st century depends on successful cooperation among like-minded partners. Collaboration among nations and between nations, the private sector and civil society is important and the effectiveness of measures to improve cyber security will require broad international cooperation.

Following are the main areas where better international cooperation is needed:[16]

1. **National nodal centres** on information infrastructure based on PPP to cooperate.

2. **Global service providers** such as Google, Microsoft, Twitter, Yahoo and Facebook to cooperate with Law Enforcement Agencies in all countries and respond to their requests for investigations.
3. **CERTs** to exchange threats and vulnerabilities data in an open way to build an early watch and warning system.
4. **Incident management** and sharing of information with a view to building an international incident response system.
5. **Critical infrastructure protection** to be aimed at by establishing an international clearing house for critical infrastructure protection to share threats, vulnerabilities, and attack vectors.
6. **Sharing and deployment** of best practices for cyber security.
7. **Creation of continued awareness** about cyber threats and international coordination as part of early watch and warning system.
8. **Acceptable legal norms** for dealing with cyber crimes regarding territorial jurisdiction, sovereign responsibility and use of force to reconcile differing national laws concerning the investigation and prosecution of cyber crimes, data preservation, protection, and privacy. Addressing the problem of existing cyber laws that do not carry enforcement provisions.
9. **Incident response and transnational cooperation** including establishment of appropriate mechanisms for cooperation. Such measures must include provisions to respond to counter cyber terrorism, including acts of sabotage of critical infrastructure and cyber espionage through information warfare.
10. **Legal enforcement agencies** to investigate cases, collect forensic evidence at the behest of other countries and prosecute cyber criminals to bring them to justice.

Chinese way of Cyber Attacks—The RSA algorithm is a type of encryption used for internet services. The Chinese attack on US Naval War College in Rhode Island in December 2006 was analysed effectively and the investigators could trace it back to central servers which was running a part of 'botnet' consisting of around 2000 computers around the world. The analysis centred on this attack suggested a huge possibility of Chinese involvement.

Industrial espionage/sabotage attacks are often conducted using the following steps:

1. Thorough analysis of infrastructure intelligence of the target organisation, mainly by open sources to determine some penetration

points. Behavioural profiles of owners of possible target computers are created. These owners are sent customised, lucrative and harmless looking email messages.

2. Such sophisticated email messages contain links or attachments which open up security loopholes and backdoors for the perpetrators to breach the organisation's network. Then malicious code is injected into the computers of the target organisation which further provides detailed information about the organisation. It also allows the hackers to command these computers using dedicated controlling servers and silently study which computer has how much preference and create more sophisticated mapping to expand their attack.
3. When computers with permissions to transfer larger amount of data without raising suspicions are located, the hackers steal the desired sensitive information they actually want.

In the RSA[17] algorithm attack case discussed above, such proficiency, resources, intelligence and sophistication could not be expected from some small organisation but from some really ambitious State power—such as China.

Certain pattern recognition elements pointed out were:

a) Infrastructure access: Breaking into the target organisation's password protected systems requires major resources.
b) Scope of attack: The RSA attack compromised 763 computers which needed prior data gathering and sophisticated email messages to lure the target users. This requires sophisticated operational infrastructure which cannot be the work of any small group.
c) Sykipot: It is a back door programme which has been one of the favourite tools of Chinese hackers since late 2006. The current levels of sophistication require tremendous and continued collective effort.
d) Identifying marks: Sykipot shows use of Chinese language in the programme writing, including remnants of information in Chinese in debug information and error messages.
e) Out of a total of 329 control servers used for controlling target computers, 299 were located in China.[18]

China and Russia have similar cyber perspectives. Their views were presented in a letter for the 'International Code of Conduct for Information Security' at the UN General Assembly in September 2012. They had put forth some major points of discontent and requirements from international efforts for cyber regulations.[19] Their discontent was over: (a) other States meddling in a country's internal affairs by supporting dissidents to its regime, under the

pretext of internet freedom; (b) the militarisation of cyber space by the US; and (c) the US and other Western countries' dominance in the governance of cyber space while neglecting the need of developing countries for fairer allocations of cyber resources.

According to China and Russia, unlike the Western approach stated above, governance and norms for cyber space should be based on:

1. The right of States to determine policies for their respective national cyber spaces.
2. The need to balance the claims for free flow of information against their potential threats to national security and social order.
3. The peaceful use of networks and restrictions on cyber weapons.
4. The equal right of all States to participate in the management of internet resources. International cooperation in dealing with network based threats to a State's security.

India's Stand at the Budapest Conference

India, posing as the most important non-aligned State at the meeting did not, however, present its position on the State's role in internet governance to the Conference. Previously, it had proposed that a UN agency be created to supervise ICANN (Internet Corporation for Assigned Names and Numbers) for administration of the internet. Pending implementation, India focused on building its own cyber security capacity. It plans to achieve this by having the State work towards creating a human resource pool of 50,000 cyber security specialists by the mode of public-private partnerships.

However, shortly after the Budapest Conference, India moved away from its earlier stance in favour of continuing the system of internet governance. Instead, it suggested that "third world countries" should be playing an active role on the various ICANN advisory committees. After the Budapest Conference, at the World Conference on International Telecommunications (WCIT) at Dubai, in December 2012 India was among the 55 States that refused to sign the new International Telecommunication Regulations (ITRs), because they give the State-centric ITU a role to supervise the internet.

India's position at the Budapest Conference may be seen in the context of fear of influence of technology control regimes which may undermine the sovereign rights of other signatory nation-states. But it does not mean that India is in favour of the Russo-Chinese stance either. There are many aspects in the agenda of the Budapest Conference which India did not agree to. For example, some articles of Budapest Convention on Cyber Crime, (which is

like a Treaty) on Mutual Assistance and Trans-Border Access of computer data are still controversial. The Cybercrime Convention Committee (T-CY) conducts two meetings every year, and still had these points on its agenda for the ninth plenary meeting in June 2013.[20] It is similar to the Comprehensive Test Ban Treaty (CTBT) when it comes to the Indian perspective towards it.

At this point, India lacks two main things. First is a comprehensive and enforced Cyber Security Policy which would include important aspects such as a precise definition of cyber threat. This must include fortifying the ICT and National Networks which need more indigenous technology, clarity in legal concepts and capacity for diverse international cooperation. Well-formed organisational hierarchies, more coordinated public-private efforts and many such aspects require better understanding and focus. Secondly, there is a need for India to evolve a credible and firm stance in international cyber relations.

The inception of the US Cyber Command (USCYBERCOM), the fifth domain of security for the US, has started a new race for building offensive capacity in cyber space. China is evolving its approach known as 'informationalisation'; the UK has gone in for Government Communications Headquarters; France led the joint effort called European National Agency for Network and Information Security (ENISA) for the European Union and such other initiatives by Russia and even North Korea, have created a momentum in developing offensive capacities in cyber space.

India still lacks on this front and as a result is a vulnerable target, instead of an organised defender. The draft National Cyber Security Policy is based on a defensive approach and response strategies, but fails to state the precise need to develop an offensive capability. Though there have been instances like counter-cyber attacks and website defacement 'games' by Indian 'White Hat' hackers, India still lacks consolidated cyber power—resources are heavily fragmented.[21]

Some Notable Examples of International Cooperation with India

US: India and the US have been in dialogue for establishing mutual ties for the enhancement of cyber security since 2011. An agreement was signed between India and the US in July 2011, for enhancing closer cooperation and timely information exchange between the countries, as well as coordination on technical and operational issues.[22] Later, in June 2013, the National Security Advisers of both India and the US met to further bilateral coordination and

to enhance mutual information sharing. The same was acknowledged in the Joint Statement after the Third US-India Strategic Dialogue, held at Washington DC, in June 2012. It was mentioned that the two countries would form a joint working group for consultations on issues and international events related to cyber space.[23] In September 2013, the CERT-In and its US counterpart, held a cyber drill under which each side would attack the other side and the other side will launch counter measures to better understand the dynamics of counter measures. This was followed by an assessment of the defensive capabilities of both sides. There is now a strong working relationship between the US Computer Emergency Readiness Team and CERT-In.[24]

UK: In 2011, the UK Government estimated that cyber crime costs the UK economy £27 billion a year, equal to more than £1,000 for every household in the country. The measures under the new UK-India cooperation deal include:

- Creating a joint task force to exchange and share information to identify and counter threats.
- Police training exchanges in "cyber forensics" and other areas of detection and enforcement.
- Regular cooperation meetings between leaders in cyber security research from academia and industry.[25]

Egypt: A MoU was signed between the Ministry of Communications and Information Technology, GoI, and the Ministry of Communications and Information Technology of the Arab Republic of Egypt, on cooperation in the area of cyber security. This MoU facilitates sharing of expertise by exchanging information on all aspects of cyber security and supporting each other in taking appropriate measures in order to prevent cyber security incidents. This intensification of cooperation in the ICT will help promote trade and the technology sector.

Japan: The Japan-India Foreign Ministers' Strategic Dialogue has been held in Japan and India alternately, each year since 2007. Japan conducted the second round of the Japan-India Cyber Dialogue and the Japan-India Maritime Affairs Dialogue in the year 2013. In response, India also would like to further deepen political dialogue with Japan by promoting the 2+2 dialogue, Japan-India-US trilateral dialogue, and the Japan-India cyber dialogue. Cooperation in the field of science and technology for development of national economies and improvement of socio-economic standards of life is necessary. Similarly,

the UK and India also share a common view, to further enhance business tie-ups in the private sector and cooperation in cyber security, as well as promotion of joint R&D and bilateral cooperation in international standardisation in ICT.

Some cases that drew the attention of the international community to cyber threats:

Estonia Cyber Attacks, April-May 2007: The attacks sharply raised the awareness for cyber security among States and decision-makers in the West. Most States immediately focused their attention on creating or developing indigenous cyber security capabilities. They contributed to the intensification of efforts to institutionalise cooperation in the field of cyber security. The NATO opened its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, in May 2008, which was accredited by October 2008. The NATO recognised cyber attacks as one of the threats existing within the contemporary security environment in its new Strategic Concept of November 2010. The NATO also committed itself to developing further abilities to prevent, detect, defend against and recover from cyber attacks, and for better integration of NATO cyber awareness, warning and response with member nations.

Israeli Attack on Syria, September 2007: Israel claimed that while the air assault under operation Orchard was aimed at Syrian nuclear facilities and programme, Syrian radars could not pick any enemy signals and hence, air defence systems could not be activated. Thus, cyber weapons proved to be a useful element in supporting the conventional military operations.

Georgia-Russia Conflict, August 2008: Georgia and Russia fought for control over South Ossetia and Abkhazia. Distributed Denial of Service (DDoS) Attacks accompanied Russian military operations. Cyber attacks targeted the Georgian Government and media websites, leading to problems related to dissemination of information to the Georgian people. The Georgian experience of cyber attacks was similar to the Estonian case.

STUXNET: Iran Related Cyber Attack: Stuxnet is a threat targeting a specific industrial control system, in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet was to sabotage such a facility by reprogramming the programmable logic controllers (PLCs) to operate as the attackers. Stuxnet is a sophisticated and specific cyber-weapon that aims to cause physical harm in sabotage mode. It is believed that it uses 'off-the-shelf codes and tradecraft' and thus, quickly and effectively disarms the target. Stuxnet perhaps caused

at least a few years of delay in the Iranian nuclear programme. Cyber security threats have psychological effects as well as physical impacts. The Iranian Government could not direct its reaction to any State due to lack of physical evidence.

States often use IT and cyber space for political, economic and other purposes such as information theft related to economic interests, stealing military and civilian technology, espionage and counter-espionage, as means of political oppression, sabotage, and subversion. All these represent new realities of cyber space that the practitioners of international relations will have to get familiar with. Negotiating and navigating through cyber space or the cyber maze in future will indeed be challenging for future diplomats.

NOTES

1. "Cyber crimes have gone up 10 fold in the past couple of years", *Rediff News*, at http://www.rediff.com/business/report/tech- cyber-crime-1600-arrested-only-7-convicted/20121211.htm (Accessed April 7, 2014).
2. "Police False Arrests in Remote Control Virus Case Criticized", at http://www.japancrush.com/2012/stories/police-false-arrests-in-remote-control- virus-case-criticized.html (Accessed April 7, 2014).
3. Sanjiv Tomar, "National Cyber Security Policy 2013: An Assessment", IDSA Comment, 2013, at http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_ stomar_260813.html (Accessed April 7, 2014).
4. "India's Cyber Security Challenge", IDSA Task Force Report, New Delhi, 2012, at http://idsa.in/book/IndiasCyberSecurityChallenges.html (Accessed April 7, 2014).
5. Ria Novosti, "Estonia has no evidence of Kremlin involvement in cyber attacks." September 6, 2007, at http://en.rian.ru/world/20070906/76959190.html (Accessed April 7, 2014).
6. Dorothy Denning, "The Ethics of Cyber Conflict" March 27, 2007, at http://faculty.nps.edu/dedennin/publications/Ethics%20of%20Cyber%20Conflict.pdf (Accessed April 7, 2014).
7. "Sit-in" or "Web Sit-in" is an act in which a group of hacktivists send queries to some pre-decided servers to get the attention of the desired party. The Hacktivist group takes the moral responsibility of sit-ins.
8. World Bank Data on internet users, at http://www.data.worldbank.org/indicator/IT.NET.USER.P2 (Accessed April 7, 2014).
9. Chandra Ganasambandam and Anu Madgavkar, "Internet rise in India: Govt should ensure faster & cheaper broadband", *Economic Times*, January 10, 2013, at http://articles.economictimes.indiatimes.com /2013-01-10/news/36258323_1_broad-based-internet-impact-internet-ecosystem-internet-penetration (Accessed April 8, 2014).
10. Debarati Roy, "63% of Indian Users Use Pirated Software", *CIO News*, May 23, 2012, at http://www.cio.in/news/63-indian-users-use-pirating-software-263522012 (Accessed April 8, 2014).
11. Verizon Data Breach Investigation Report, at http://www.verizonenterprise.com/DBIR/2013/ (Accessed April 8, 2014).

12. National Cyber Security Policy Draft of March 2011, http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf (Accessed April 8, 2014).
13. Ministry of External Affairs, Government of India, "Joint Statement on Cooperation between India and the UK on Cyber Issues", November 8, 2012 at www.mea.gov.in/bilateral-documents.htm?dtl/20792/Joint+Statement...C.. (Accessed April 8, 2014).
14. *The Cyber Commander's eHandbook*, at www.technolytics.com/Cyber_Commanders_eHandbook_F_2013.pdf (Accessed April 8, 2014).
15. Roger Hurwitz, An Augmented Summary of Harvard, MIT and University of Toronto Cyber Norms Workshop, October 19-20, 2011, Cambridge MA, at ecir.mit.edu/index.php/research/working.../294 (Accessed April 8, 2014).
16. Kamlesh Bajaj, 'The Cybersecurity Agenda, Mobilizing for International Action', East-West Institute, at http://wwwewi.info/system/files/Bajaj Web.pdf (Accessed April 8, 2014).
17. RSA stands for the asymmetric cryptographic algorithm named after Ron Rivest, Adi Shamir and Leonard Adleman, the inventors of the software algorithm.
18. Gabi Siboni, "What Lies behind Chinese Cyber Warfare", *Military and Strategic Affairs*, Vol. 4, No 2, September 2012, at www.inss.org.il/index.aspx?id=4538&articleid=2560 (Accessed April 8, 2014).
19. Timothy Farnsworth, "China and Russia Submit Cyber Proposal", Arms Control Association, at http://www.armscontrol.org/act/2011_11/China_and_Russia _Submit_Cyber_Proposal (Accessed April 8, 2014).
20. Cybercrime Convention Committee (T-CY) 9th Plenary, Strasbourg, June 5, 2013, at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_er (Accessed April 9, 2014).
21. Techgig News 'How prepared is India for cyberwar', *Tech News*, March 2013, www.techgig.com/tech-news/editors-pick/How-prepared-is-India-for-cyberwar.. (Accessed April 9, 2014).
22. "United States and India Sign Cyber Security Agreement", Press Release, Embassy of the United States, New Delhi, July 19, 2011. See http://newdelhi.usembassy.gov/pr071911a.html (Accessed April 9, 2014).
23. Joint Statement on the Third U.S.-India Strategic Dialogue, Press Release, June 13, 2012, at http://www.state.gov/r/pa/prs/ps/2012/06/192267.htm (Accessed April 9, 2014).
24. Manan Kumar, "India ties up with US for cyber security", *DNA News*, New Delhi, September 13, 2012, at http://www.dnaindia.com/india/report_india-ties-up-with-us-for-cyber-security_1740178 (Accessed April 9, 2014).
25. James Kirkup, "David Cameron to strike cybercrime deal with India", *The Telegraph*, February 19, 2013, at http://www.telegraph.co.uk/news/politics/9879272/David-Cameron-to-strike-cybercrime-deal-with-India.html (Accessed April 9, 2014).

6

Climate Change and International Relations

Global Warming and Climate Change: An Introduction

Nature has had its own mechanism of keeping the earth surface temperature within comfortable limits for human civilization to survive and progress. However, over the past five to six decades, modern industrial activities have caused a steep increase in Greenhouse Gases (GHG) in the atmosphere, trapping the heat on the earth surface and causing global warming. While natural climate variations have existed for millennia, anthropogenic climate changes since the world wars and the fast pace of industrial revolution, are the main causes for accelerated warming of the earth's environment and its adverse effects on a global scale.

Nine of the ten hottest years on record were in the past twelve years. In recent months, extreme rainfall and floods have affected all parts of the world from the Mississippi Valley, to Kedarnath in the Himalayas, and the US' east coast (Super-storm Sandy) devastating human lives and causing tens of billions of dollars in damages. Climate change is already happening and affecting the daily lives of thousands. Our planet is heating-up and carbon pollution from fossil fuel based energy is sending heat-trapping emissions daily into the air. About 90 million tons of carbon pollution enters the atmosphere every day. That means a hotter world for all of us now, in coming years and a very hostile and unstable environment for the next generation, in the future.

As of end 2012, the earth was already nearly 0.8°C warmer than the pre-industrial temperature that had stabilised over thousands of years. The rate of carbon dioxide (CO_2) emission is already an order of magnitude higher than what nature can absorb. The consequent climate changes are thus already perceptible in terms of increasing incidents of extreme weather, glacial melting and floods in some regions and hurricanes, droughts, forest fires in other regions. Compared to the pre-industrial level of 280 ppm (parts per million) of CO_2 concentration in the atmosphere, the level crossed 400 ppm in May 2013. Continued increase can soon disturb the environment to a point of no return, when the feedback systems of nature may be overtaken and our environment subjected to irreversible changes.[1]

GHG emissions in the earth's atmosphere linger for several decades. Hence, climate change is a slow and invisible process, effects of which may manifest after several years. The impact of climate change will be different across different parts of the world and actions of one country can harm the vital national interests of another. Historically, 20 percent of the world population in developed countries has consumed 80 percent of the global energy resources and is thus responsible for 80 percent of CO_2 emissions. But the adverse effects of climate change will be far more serious on more populous and developing countries of the world. The resultant stresses that this can produce in societies, are now recognised as a potential cause for the next major war among nations. Managing climate change will therefore require cohesive global action which cannot be achieved without effective international coordination for mitigation efforts. But views of different nations are presently very divergent about WHO should do WHAT and by WHEN, and this has become an important issue for international relations (I.R.) and diplomacy.

The United Nations (UN), in recognition of the dangers of climate change to humanity, has convened several international conventions in the past three decades, to debate on how best to arrest the undesired changes in the atmosphere; but a universal consensus among all sovereign countries for an effective solution to this problem of global dimensions is still not in place. The main cause of anthropogenic global warming is of course the heavy dependence on carbon fuels for electricity generation and transportation all over the world. The energy needs of modern society have been increasing steadily and by 2050 the global energy requirement is expected to be about 45 percent higher than the 2010 level. If effective measures are not put in place urgently, we are looking at over 40 percent more CO_2 in the atmosphere and over 2°C rise in average temperature by 2050. Serious investments are

needed to quickly improve the efficiency of energy usage and for a rapid shift away from fossil fuels to greener, renewable energy resources all over the world.

If effective measures for rapidly arresting global warming are not in place by 2015, there will be obvious major economic costs for managing serious consequences of escalating climate change and increasing natural disasters by 2025 and beyond. Who will pay how much for saving the environment is a very contentious issue that will require clear scientific understanding of the issues and astute diplomatic capabilities for achieving binding global agreements for effective mitigation of global warming before it gets too late. Science and technology (S&T) will invariably play a pivotal role in helping to win the battle of climate change and also for providing practical solutions for sustainable development in the future.

Arriving at a global consensus on climate change presents one of most important diplomatic challenges of our time. Impact of climate change on national security perceptions are very significant and even regional cooperation for joint action is not easy to achieve, because the potential cost of mitigation or disaster management is different for different countries. As time runs out for avoiding the 'tipping point' of climate change, international tensions will escalate with the increasing frequency of natural disasters. A common logic for common good must thus overtake individual national priorities. The next 10-15 years will probably present one last opportunity for each nation to maximise its scientific and diplomatic potential towards protecting nature through collective global action.

Climate change is the defining issue of our times. It is perhaps, the greatest challenge to sustainable development. It should be addressed by all countries with a shared perspective, free from narrow and myopic considerations. Developed countries need to look beyond their narrow self-interests and work jointly with developing countries to evolve cooperative and collaborative strategies on the issue of climate change, which is of immense relevance for the future of mankind. However, efforts so far in the direction of meeting the challenges of climate change have been sporadic and incoherent. We urgently need a new economic paradigm, which is global, inclusive, cooperative, environmentally sensitive and above all scientific. According to Jeffrey Sachs, a leading economist and proponent of sustainable development, "The world's current ecological, demographic and economic trajectory is unsustainable, meaning that if we continue with business as usual we will hit social and ecological crises with calamitous results".[2]

Sustainable development models based on addressing the needs of the poor and for optimal harnessing of scarce resources of water, air, energy, land and biodiversity will have to be developed through more cooperative endeavours, so that we can make some headway in saving our lone planet from the brink of climate disaster.

This chapter presents a fairly comprehensive look at the status of global warming and climate change in the context of how human development has taken an unsustainable route to progress and how international cooperation will be crucial to limiting the damage. Energy and environment issues are discussed in detail to highlight the dilemma of contradicting priorities and the impact of climate change on national security, including energy, water and food security. The focus will be on how S&T can be leveraged to resolve climate change concerns through concerted international dialogue and cooperation.

The complex dimensions of international dialogue are reviewed to bring clarity to Indian priorities for setting goals for climate negotiations to protect India's national interests. This has to happen while also contributing to global efforts for mitigating global warming and adapting to adverse effects of climate change. The next few years will offer an opportunity for finding an Indian solution for a global problem through sound application of technology and diplomacy. India will have to walk a tightrope in garnering collective global momentum to avoid a climate catastrophe. In this challenge S&T can not only empower the climate negotiators with comprehensive information, but also help them in arriving at diplomatic agreements with other major players that can hugely impact Indian interests.

Understanding the Basics

The earth's atmospheric temperature depends on the balance of energy entering and leaving the planet's atmosphere. When incoming energy from the sun is absorbed by the earth system, the earth warms-up and when the sun's energy is reflected or released back into space, the earth cools. Many factors, both natural and man-made can cause changes in the earth's energy balance. Nature has its intrinsic capacity to adjust to minor changes in maintaining this temperature balance for life to survive. Variations in the sun's energy reaching the earth and changes in the earth atmosphere or earth surface in terms of absorption or reflection characteristics are the main components of this delicate balance of heating and cooling the planet. Scientists have put together various models of the earth's climate, going back to thousands of years, by analysing

a number of indirect measures of climate parameters such as ice cores, glacier volumes, forest covers, pollen remains, natural greenhouse effects and ocean temperature patterns etc. including even the variations in the earth's orbit around the sun.

Over the last 100 years, and particularly during the last five decades, the eco-balance of nature has been disturbed by excessive industrial activities and by the growing population on earth. The human imprint on the global environment has now become so large and active that it rivals some of the great forces of nature in its impact on the ecosystem of the earth. Tracing the history of the evolution of the 'Anthropocentric' world (human activity dominated) since the industrial revolution, one can easily see the cause and effect pattern of environmental degradation. The evolution and scale of human activities, as we move into the 21st century, has caused profound changes to our relationship with the living world and the large geophysical cycles that drive the earth's climate system. Thus 'Anthropogenic' effects need to be recognised as the new catalyst of change in the earth's history. Human activity is also significantly altering several other biogeochemical factors or element cycles, such as nitrogen, phosphorus or sulphur that are fundamental to life on earth.

Greenhouse Gases (GHG) are those that allow the sun's radiation to warm the earth surface but prohibit the reflected heat in the infrared band from escaping back to space, because the layers of lingering, invisible GHG clouds reflect the heat released by the earth back to the earth. This heat trapping effect causes warming of the earth in a slow but cumulative process as the GHG clouds once created, linger in the atmosphere for decades, resulting in rise in temperature, which in turn causes the climate to change years after the GHG are emitted. While weather changes can occur very fast and seasonal changes are relatively slow, climate changes are very slow and have long-term impacts. Our average earth temperature is already over 0.8°C hotter than pre-industrial levels and the adverse impacts of climate change due to GHG emissions of the past 4-5 decades are already beginning to manifest in the form of extreme and unpredictable weather events that are more frequent than ever before in history.

Of the many components of atmospheric gases only some gases block heat from escaping. Of these, some like water vapour are seen as 'feedback agents' because it helps nature to self-adjust to natural temperature changes. Water vapour increases as the earth's atmosphere warms, but so does the possibility of clouds and precipitation that tend to cool the atmosphere. Several

other gases that do not respond to natural changes are described as 'forcing' climate change as they disturb the balance of nature.

Such Greenhouse Gases are:

- Carbon dioxide (CO_2)—CO_2 is absorbed and emitted naturally as part of the carbon cycle, through animal and plant respiration, volcanic eruptions and ocean-atmosphere exchange. Human activities, such as the burning of fossil fuels and changes in land use, release large amounts of CO_2 in the atmosphere. Humans have increased atmospheric CO_2 concentration by 40 percent since the industrial revolution began. This is the most important long-lived gas and the 'forcing' mechanism of climate change.
- Methane (CH_4)—This hydrocarbon gas is produced both by natural sources and human activities, including the decomposition of wastes in landfills, rice cultivation, as well as ruminant digestion and manure management associated with domestic livestock. On a molecule-for-molecule basis, methane is a nearly 20 times more active GHG than CO_2, but it is much less abundant in the atmosphere.
- Nitrous oxide (N_2O)—This is another powerful GHG produced by soil cultivation practices, especially the use of commercial and organic fertilisers, fossil fuel combustion (like automobile exhaust), nitric acid production and biomass burning. Certain industrial wastes often emit sulphur fluoride gases.
- Chlorofluorocarbons (CFCs)—These are synthetic compounds entirely of industrial origin used in a number of applications. These are now largely regulated in production and release to the atmosphere by international agreements because of their ability to contribute to the destruction of the ozone layer. They are also GHG.

Most of these GHG are by-products of human activity and the most serious component is the CO_2 emission from burning carbon-based fuels for electricity generation, transportation requirements and industrial activities—all being intrinsic to human development. However, since the process of global warming is very slow and invisible by itself, realisation of warming is evident only by the actual increase in average temperature. Unfortunately, by this time, the GHG clouds that cause this temperature rise are already there in the atmosphere for the next few decades. This slow and invisible process has now gone beyond the self-adjusting capacity of nature and hence, we are now in a phase of cumulative build-up of GHG clouds that will affect the earth's climate for decades and perhaps centuries to come.

Status of Global Warming

Human development has indeed led to a rapidly increasing wealth of knowledge upon which humanity has evolved as a complex civilization that continues to increase its power by manipulating the environment. Exploiting fossil fuels in pursuit of development and security has enabled mankind to undertake new activities and vastly expand and accelerate existing activities, consuming more fossil fuels and emitting more GHG. Between year 1800 and 2000, the human population grew 6 times—from about one billion to six billion, while energy use grew by about 40-times and economic production grew by 50-times. The atmospheric CO_2 concentration was 277 ppm in 1750, growing to 283 ppm in 1800 and 284 ppm in 1825. All this increase was well within the range of nature's capacity to absorb and balance GHG in the range of 260–285 ppm by self-adjusting natural feedback mechanisms.

Changes in the earth's environment have been dramatic since World War II and this period from 1945 to 2000 represents the period of 'great acceleration' in atmospheric degradation. World population doubled from 3 to 6 billion in this period, while the leap in economic activity was 15-fold and petroleum consumption grew by a factor of 3.5 times. Atmospheric CO_2 concentration grew from 310 ppm in 1950 to 369 ppm in 2000, it further increased to 390 ppm by 2010 and it crossed 400 ppm in May 2013. Besides this steep increase in CO_2 concentration there have also been other significant pollutants as discussed above.

The 'great acceleration' of industrial activity between 1945 and 2000 was almost entirely driven by the Organisation for Economic Cooperation and Development (OECD) countries that represented only 20 percent of the world population, while the balance 80 percent, mainly in the developing countries, contributed less than 20 percent of the cumulative CO_2 emissions. However by 2008-2010, coal and oil became the main fossil-fuel energy sources for the rapidly developing economies like China and India that now account for the major rate of increase in CO_2 emissions.

The IEA (International Energy Agency) forecasts that oil production could increase by 26 percent by 2030, to avoid reaching the peak point, but the prospects of achieving this level within two decades, at affordable prices, are dim. Hence, peak oil can be estimated to happen by 2025. But now there is increasing expectation that heavy oil and shale gas extraction from deep underground by fracking techniques can off-set peak-oil problems. However, the impact of such deep fracking and heavy oil production on water resources and bio-diversity is fairly grave. The irony is that if heavy oil and shale gas is

produced at affordable cost, it may perpetuate dependence on fossil fuels and actually accelerate global warming to the tipping point. It would also hurt the momentum for shifting to renewable energy which can stop further degradation of the atmosphere. Climate change will probably entail a heavy economic penalty in the future, far in excess of the investments needed today for rapid expansion of renewable technologies to slow-down global warming. Unfortunately, this foresight is yet to be accepted by the development hungry society that is compromising future generations of humankind.

Ironically, mankind is now contemplating geo-engineering solutions to artificially cool the earth but there is no doubt that if geo-engineering is to play a significant role in preventing the climate system from warming beyond the 2°C guardrail, much more scientific research is required and serious mitigation work is needed. Our world seems destined to enter its sixth great extinction event unless urgent steps are taken now![3]

Studies show that solar variability has played a role in climate change in the past causing the 'Little Ice Age' between approximately 1650 and 1850, when Greenland was largely cut-off and glaciers advanced in the Alps. However, evidence shows that current global warming cannot be explained by changes in energy from the sun alone. Since 1750, the average amount of energy coming from the sun has either remained constant or increased very slightly. Scientists have also observed cooling in the upper atmosphere and warming in the lower parts of the atmosphere. This is because GHG are trapping heat in the lower atmosphere. Climate models that include solar irradiance changes, can't explain the observed temperature trends over the past century without including an additional rise in GHG due to non-natural or man-made reasons.[4]

The fourth assessment report of the Inter-governmental Panel on Climate Change (IPCC) in 2007[5] has affirmed the gravity of the problem of adverse climate change and raised some important issues that may be summarised as follows:

- While natural forces have always influenced the earth's climate (and always will); human-induced changes in the levels of atmospheric GHG are playing an increasingly dominant role in the observed changes in global climate.
- After considering the influences of the known causes of climate change—natural and human-induced, the significant increase in average global temperatures over the last half century, can be attributed to human activities with a certainty of more than 90 percent.

- The rise in temperature has already affected various natural systems in many global regions and hence, some adverse future changes to the climate are inevitable, unless immediate steps are taken to arrest and reverse the trend.

Global warming due to increasing concentration of GHG in the atmosphere is a slow but cumulative process. Nature's feedback processes—a hotter earth causing more greenhouse effects and more warming—can intensify beyond a 2°C rise over the average temperature of past 1000 years. This can lead to the tipping point of global warming when irreversible processes can go beyond the control of human civilisation. The consequences of changing the natural atmospheric greenhouse effects are difficult to predict exactly, but certain effects seem very likely. As the earth gets warmer, some regions may welcome warmer conditions but others may not. Warmer conditions will lead to more evaporation and precipitation overall, but individual regional effects would vary—some becoming wetter and others dryer. A stronger greenhouse effect will warm the oceans and partially melt glaciers/ice-sheets, increasing sea levels. Ocean water will expand if it warms, contributing to further rise of sea levels.

Carbon dioxide concentration of 400-440 ppm corresponds to a 2.4°C rise in global mean temperature. When the 2°C mark is crossed, natural positive feedback processes could accelerate further warming, leading to non-reversible climate changes. Melting of Arctic ice-caps would reduce the reflecting surface areas, thus absorbing more heat and causing more melting in a feedback cycle. Consequent flooding and sea level rise can have a severe impact on availability of habitable land, drinking water, food production and can lead to an increase in vector borne diseases. Once the ice-sheets start melting, exposing the northern permafrost, they can release Methane (CH_4) which is 20 times more harmful than CO_2. Such eventualities can exacerbate global warming to levels beyond exacting analysis and forecasting. Hence, it would be better to err on the side of caution.

Increased evaporation from oceans and land will contribute water vapour to the atmosphere, which will lead to further trapping of heat and also change precipitation patterns. Tropical regions will get affected much before the higher latitude regions. At 3°C rise, Arctic ice-caps would disappear completely and Amazon rain-forests could dry-up into deserts, drastically reducing earth's capacity to absorb CO_2 emissions. At 4°C rise, Antarctic ice-sheets could collapse totally, flooding low-level coastal cities world-wide. New deserts would spread across the world, including Europe, with death and destruction due to extreme climate conditions. At 5°C rise, searing heat waves would make

sub-tropical regions unliveable, forcing hundreds of millions of climate refugees to move-out, searching for food and water. At 6°C rise in temperature, huge inhabitable areas would span the globe causing mass extinction of natural life and the earth's ecosystem will be changed permanently![6]

The above scenario looks very likely in the next 150 years, unless urgent steps are taken at a global level to effectively slow-down global warming in the next 10-15 years. Delay in action could actually cost billions more per year to save the earth's eco-balance, besides having to suffer adverse consequences. Considering the inescapable reality of the continuing use of fossil fuels for global energy requirements in the near future, it is of vital importance to adopt a complete range of carbon mitigation measures including CO_2 sequestration by major global forestation drives and other technology means. The next few years up to 2025, could be the last window of opportunity for mankind to prevent catastrophic changes in the earth's atmosphere. Game-changing policy initiatives are needed for quick and decisive global action. This is the greatest challenge for experts managing international affairs.

It is important to understand why this runaway situation looks difficult to avoid. Modern society is hungry for energy for development and security needs in the immediate future. The increasing global population, combined with the aspirations of millions joining the lifestyles of the developed affluent society, will cause global energy needs to grow faster than our capacity for providing clean and sustainable energy. The result is the growing use of coal, oil and natural gas reserves that is creating alarming levels of GHG. Slowing down this human development activity has such obvious economic and lifestyle costs, that no one is yet ready to compromise development in the larger interest of the environment.

It is only in the past 15-20 years that warnings by climate scientists are beginning to be heard, and a realisation is dawning that the cost of not slowing down global warming now—within the next 10 years—will actually cost much more in addressing the consequences in the future. By some conservative estimates, every dollar invested now in green and renewable energy technology could save over $ 3 over the next 10 years. Therefore, the urgency of climate change mitigation action and the associated costs are becoming more understandable and acceptable for modern society.

Mitigation of global warming and management of climate change is a problem of global dimension, but different countries have contributed to the problem in vastly varying levels and the adverse effects of climate change will

also be different for different geographic regions and countries. Hence, finding a global consensus for concerted efforts is posing a major diplomatic challenge. While each country is protecting its own priorities in terms of development and economics, time for convergence on collective action is slipping away, with carbon concentration in the earth's atmosphere fast approaching threshold levels with irreversible effects.

Success or failure in managing climate change and its consequences will be a major factor in international relations among countries big or small, rich or poor.

Energy and Environment Dilemma: Indian Priorities

Inherent Dilemma and the Basic Issues

Since World War II, our world has been witness to rapid industrialisation with increasing use of energy derived from fossil fuels whether it is for electricity generation or transportation. The more the energy consumption using carbon fuels, more is the CO_2 emission in the atmosphere that causes climate changes creating unpredictable and extreme weather events. There is now a sober acceptance that GHG emission due to human activity is almost of a magnitude higher than the natural and this clearly needs to be reduced to a level that nature can absorb, without getting hotter, to avoid a runoff situation. But reducing CO_2 emissions, all else remaining the same, would mean using less energy and that amounts to slowing down economic progress or investing in more expensive but non-polluting energy options. Therefore, the basic dilemma is—how to balance increasing energy needs with the need to reduce carbon emissions. The earth has clearly entered a new 'age of consequences', where the national priorities of economic progress and human development are getting into conflict with the need to care for the environment which requires serious mitigation of global warming and serious efforts to preserve the delicate ecosystem.[7]

Developed countries have been almost entirely responsible for the anthropogenic CO_2 emissions in the atmosphere, due to which the entire earth and particularly the poorer developing countries, will face adverse consequences. Until a global consensus can be reached about which country will reduce how much emission and by when, the earth will continue to get warmer with serious climate change impacts for future generations. For every sovereign nation, the dilemma about how best to avert the emerging threat

to human security due to climate change while balancing the interests of energy security and development priorities, is also a national security challenge.

The dilemma is more acute for a country like India, as it struggles to carry its billion plus population to participate in the quest for its long overdue economic development. To stay on a rapid growth trajectory, India may require five or six times more energy by 2030 than what it consumed in 2010. Demand for energy in China, Brazil and many other fast developing economies, is also rising steeply. Industrially advanced countries that used vast amounts of energy during their own development years, are now concerned that rising energy consumption in the fast developing countries, can push global warming to a point of no return. The fast developing countries with a rising need for energy, are now asking the developed countries to reduce their energy demands and significantly reduce their carbon footprints to allow a fair share of energy for growing economies.

The second part of the dilemma is, how should nations agree on equitable distribution of the limited global energy resources and how humanity as a whole must contain global warming to prevent catastrophic climate changes? On the one hand, world energy shortages can trigger major tensions, conflicts and even war, and on the other, unprecedented climate changes can cause clear danger to regional and international stability. The resultant consequences combined or singularly, could pose a grave threat to the national security of individual sovereign nations, particularly so, for developing nations in regions that are already under various stresses.

The dilemma for India has several unique characteristics. India has good coal reserves, but the quality of coal is very poor. Hence, increased use of low-quality coal can alarmingly increase the carbon signature of the country. Modest reserves of natural gas are yet to be tapped fully and pricing has become a political issue. Almost all oil requirements are met from imports and the combined energy import bill today accounts for over 80 percent of national imports. Such a heavy dependence on imports can have major concerns about vulnerabilities and India therefore, has been investing in hydropower as well as nuclear power. Hydropower is already contributing about 18-20 percent of the energy requirement and the potential for large hydro-power now looks limited. Nuclear energy contribution has been stagnating at about 3 percent and ambitious plans of increasing this to over 10 percent are stalled due to public perceptions of safety, particularly since the Fukushima accident in Japan. Renewable energy options continue to be more expensive and investments needed for boosting this sector are not yet forthcoming, due to the absence

of a supportive policy framework and lacklustre implementation of existing enabling policies. India also lags behind in energy efficiency performance when compared to many industrial nations. There is thus an urgent need for an integrated energy policy for India.

Given the increasing global concerns of climate change and domestic imperatives for supporting a fast growing economy, Indian policy makers have a tight rope to walk. Domestically, there is urgency for improving energy efficiency across all sectors and for rapidly increasing the share of renewable sources in the energy basket. At the same time, India needs to be competitive in seeking access to external energy sources in the immediate future and attracting international investment for focused research and development (R&D) to enhance energy performance and move to renewable energy sources.

Simultaneously, India must actively engage in the international dialogue for mitigation of global warming because India will be one of the worst affected nations by climate change induced extreme weather conditions, natural disasters and climate refugees. While India must try its utmost to not allow its carbon signature to grow beyond a point, it will be a major challenge for Indian diplomacy to convince world powers that the Indian problems are not entirely of India's making and hence, global players must share the cost of urgent actions needed in India.

India will need substantial investments for introducing renewable energy sources in a big drive in the next 5-10 years, particularly from solar, wind, bio-gas and small hydro. Until newer technologies to help harness these sources become well established and cost competitive, India will need to enhance its share of nuclear energy from 3 percent to about 10 percent to tide over immediate energy shortages. Many among the developed world can afford to move away from nuclear energy due to public perceptions of safety, because their future needs are already being met from existing technology options. Such advanced nations are looking at renewable options for reducing their carbon signature. The case for India is different in the sense that the demand-supply curve for India is nowhere near the plateau and hence, renewable energy sources are urgently required for bridging the gap between demand and supply with as little carbon penalty as possible. For India, renewable energy is not an option but a necessity.

Global Energy Scenario

The world's population crossed the 7 billion mark in October 2011 and the average global energy consumption rate was about 15 terawatts (15×10^{12}

Watts). Roughly 78 percent of this energy was consumed by the industrially advanced countries and the balance 22 percent was consumed by 80 percent of the population in developing countries. A quick look at the global energy scenario shows that in terms of energy consumption, China with 20.25 percent of world consumption has already overtaken the US (19.04 percent). Russia is third at 5.75 percent while India is fourth at 4.36 percent, followed by Japan (4.24 percent), Germany (2.65 percent), Canada (2.63 percent) and France (2 percent). However, comparing the same eight nations in terms of per-capita consumption, Canada is one of the highest with 8300 'Kg of oil equivalent' (koe) with the US right behind at 7795 koe. Next are France at 4615, Russia at 4423, Germany at 4203, Japan at 4040, China at 1652 and India at 512. It is interesting to note that although India ranks as the fourth largest energy consumer in the world, its per capita consumption is very low, less than 1/10th of the US or Canada and about 1/4th of the world average.[8]

Unfortunately, much of the energy needs of the industrialised world are met from fossil fuel resources that have been most cost-competitive but also heavy emitters of GHG. As global demand for energy threatens to overtake the supply of these fuels, the increase in prices becomes inevitable in driving economic competition to an even higher pitch. Thus, with no let-up in global warming, the imminent consequences of a hotter earth will have more severe impact in highly populated developing countries than advanced nations with lower density of population and better infrastructures.

World energy consumption is expected to grow by 45 percent by year 2035 and with the 'business as usual' model the global emissions of GHG are also expected to increase by about 42 percent by the year 2035. However, if dependence on carbon fuel is reduced drastically and the share of clean energy sources is improved to nearly 50 percent from the present 15 percent, further global warming could be mitigated significantly. There is therefore a need for technological innovations and investments in clean and renewable technologies including techniques for carbon sequestration at affordable cost. The penalty of not achieving the above could mean painful cuts in future energy usage that could slow-down economic progress or accelerate environmental disasters that could spiral out of control and threaten human well-being and even survival.

As brought out by Thomas L. Friedman in his book, '*Hot, Flat and Crowded: Why We Need a Green Revolution—and How It Can Renew America*' our world is indeed getting hotter than ever before due to our insatiable hunger for energy, and comforts of mankind. An increasing number of people globally

are graduating to middle class aspirations that are very energy-dependent. Global resources being limited, this will inevitably increase the sense of vulnerability between societies and countries. Asia in the year 2000 had 60 percent of the global population, producing 40 percent of the global Gross Domestic Product (GDP). By 2020, Asia may support 50 percent of the population but produce 60 percent of global GDP. Hence, the centre of focus is shifting and what happens in Asia will affect the world very significantly. Political consequences of this shift could prove very stressful for global stability and peaceful coexistence. This presents a huge challenge and an opportunity for Indian diplomacy to make the best use of the opportunity for projecting India's rising role in international affairs.

Global warming is cumulative and hence concerns and dangers will increase exponentially. The impact on economy and lifestyle will create conflicts among individual countries that will try to preserve their respective values and priorities. It should therefore be very clear that the politics of energy will shape world power equations in future. Energy shortages and common dangers of climate change will compel nations to redefine national priorities. Nations will have to learn to compete and cooperate at the same time, or go to war over climate change!

The well known Stern Review of October 2006 on "The Economics of Climate Change,"[9] argues that the world needs to invest one percent of global GDP each year to mitigate the effects of climate change, through raising the price of carbon and by investing in improving energy efficiency as well as harnessing alternative energy clean resources. If this is not done, the Review argues, up to 20 percent of global GDP may be lost eventually because of the damage done by global warming. Quite clearly, energy security can no longer be separated from effects of climate change and one must worry about effective global energy management over and above the priorities of individual nations. The IEA predicts that the world's total energy usage may increase by more than half the present level over the next 25 years and use of coal for power generation may predominate over other means, thereby causing serious concerns of runaway conditions of climate change.

The US has for decades been the world's largest CO_2 emitter but by 2008 it was reported that China overtook the US in total emissions although its per capita emissions remains much lower in comparison. Coal being in abundant supply in the US, China and India, the tendency to rely more on coal seems unavoidable, but it will be imperative to replace the present polluting technologies with clean-coal technologies for future power

generators, in order not to exacerbate global warming. The world today is debating on how much of this cost of shift to new technologies should be supported by the advanced nations that have already secured their energy security issues through easy access to cheap fossil fuels, when global warming was not a serious issue.

It is expected that the Organisation of the Petroleum Exporting Countries (OPEC) share of the global oil market may grow to over 50 percent. The era of an oil-price controlled economy is already in play. It may be interesting to observe that while global warming concerns are major drivers for investments in energy efficiency technologies and for renewable energy technologies, the oil producers—particularly the OPEC countries—stand to lose out if that succeeds. Hence, the OPEC will be the last to encourage green energy investments and will always try to control the price of oil to keep oil supply at a competitive rate, for slowing down investments in such technologies which would reduce dependence on oil. It is therefore paradoxical that if there should be a 'war-risk' environment driving up oil prices, that would actually make alternative energy development more cost-effective, thus contributing to better mitigation of global warming effects. The world may therefore witness an interesting play of forces of economic and security priorities balancing each other, in the process of managing GHG emissions.

Inadequate energy supply or highly import-dependent energy supply can be a serious threat to national security because the country remains vulnerable to external forces and priorities. Oil and coal are expected to peak well within the next few decades and the cost of oil and coal will be on a constant rise—as is already happening. Energy security is therefore one of the top priority security agendas for India and most other progressive nations. Several developing nations on fast-track development are bound to need more energy from every source possible and this will have a major impact on the dilemma of how to balance increasing energy consumption with the need to contain global warming.

It is therefore a no brainer that for all nations, enhancing energy efficiency and increasing the share of renewable clean energy produced within the country, will be an absolute imperative. For every nation, the ideal energy policy for the future must include a wide mix of renewable energy options—solar, wind, hydro, biomass, nuclear etc., to reduce dependence on carbon-based energy sources that are not sustainable. The energy policy must also include investments in innovation for major improvement in energy efficiency

and for exploring new resources, such as gas hydrates, tidal waves, controlled thermonuclear fusion as well as other new technology options.

It is evident that competition for coal, oil, natural gas and uranium will get hostile as nations jostle to ensure own energy security despite depleting global resources. Per capita electricity consumption of India was 733 kWh by end-2011. In comparison, the numbers for other major consumers are: the US—13,994, Europe—6,009, China—1,750 and the world average per capita stands at 2,596 KWh. At the same time, carbon footprints in MMT/year (per capita) are—the US 17.62, Russia 12.55, Japan 9.26, China 6.52 and India 1.45 MMT/year. But in terms of total carbon footprint already China is number one at 8715, with US—5490, Russia—1788, India—1724, Japan—1180. If China and India reach world average per capita electricity consumption, they will perhaps be the worst polluters of the environment; unless their energy mix changes drastically in favour of renewable. Hence, the energy and environment performance of China and India are under close watch of the international community![10]

The global alternative policy scenario presented in the *World Energy Outlook 2006* of the IEA shows how the global energy market could evolve if countries around the world were to adopt policies and measures currently under consideration for reducing CO_2 emissions and improving energy supply security. In the given scenario, the share of renewables in global energy consumption remains largely unchanged while the share of traditional biomass falls. Hydropower production may grow but its share will remain stable, while the share of other renewables (including solar, wind and geothermal) will increase most rapidly, but they may still remain a small component of the overall energy scenario in 2030. The world will continue to be dependent largely on fossil-fuels. This is not a happy situation for mankind.

Energy Security: Indian Perspective

The concept of national security is now changing to encompass everything that can affect national interests including the security, aspirations and potential of its people. Comprehensive National Power (CNP)—is not only about protecting national interests but goes beyond, in terms of ability to influence global decisions. For every nation, energy security and sustainable development will be critical to enhance the CNP level, so that it can become a global player based on its CNP strength. India's Integrated Energy Policy (IEP) approved in December 2008, envisions a road map for sustainable growth with focus on energy security in the future. Until 2012 India's

electricity production was dominated by fossil fuel at 74 percent and hydropower at 15 percent, while renewable energy—mostly wind and solar, provide 8 percent and nuclear power accounts for 3 percent. But in recent years contribution of wind and solar has been rising promisingly.

Given that the peak oil phenomenon can be expected within the next 10-20 years, prices could spiral upwards and the era of cheap oil seems to be over. While for many advanced countries energy demands have already reached a plateau, energy demands for India, on its fast growth-curve are going to rise significantly. Hence, the most important issue for India is to draw up a plan to combat the effects of peak oil through exploitation of every other energy source. The 'Integrated Energy Policy' (IEP) is about defining a viable energy strategy, which can translate into long-term energy independence for the nation. In fact, as renewable energy gets competitive with carbon fuel, a whole new dynamic will open up to affect the politics of oil pricing and influence international affairs.

Improving energy efficiency and promoting distributed energy generation on a war-footing are clear priorities for India; where energy thefts alone account for over 20 percent loss. Reducing transmission and distribution (T&D) losses to a minimum can save another 15 percent of electrical energy. The industrial sector in India is responsible for about 50 percent of total commercial electricity consumption. Small and medium-sized enterprises (SMEs) have big potential for increasing energy efficiency using technology upgradation. Policy incentives and strengthening of the Bureau of Energy Efficiency for strict monitoring of electricity wastage can improve energy efficiency and reduce domestic energy demand by about 30 percent, across industrial and domestic sectors.

The importance of renewable energy sources as well as nuclear energy technology needs to be appreciated in the above context, particularly for a country like India which has very poor self-sufficiency in energy and which is also on a path of steep economic progress, requiring more and more energy. Priorities for India therefore, must include a variety of initiatives to strengthen its energy security. At the same time, policy makers should be mindful about not worsening the global warming situation.

Increasing the strategic reserves of oil, improving the efficiency of present oil usage, both in power generation and the transportation sector, and investing in the search for more oil and gas reserves within the country, are clear priorities for the short term, where government policies must create major incentives and very focused coordination. Investments in clean coal technologies and

for renewable energy technologies must also increase, so as to reduce the dependence on carbon-based energy in the long term.

India also needs the political maturity and pragmatism to realise that nuclear energy must be harnessed to a larger extent in the interest of energy security as well as environmental concerns. India needs an opening like the India-US nuclear deal to break out of the technology embargo regimes and become an international partner in nuclear energy technology. With technology advances helping to minimise the traditional risks associated with nuclear reactors, and with emerging revival in the nuclear energy option, India is very well positioned to quickly build on its indigenous nuclear energy technology expertise and become a world-class player in the nuclear energy market.

Common concerns of global warming and climate change have finally provided an opportunity for nations to cooperate in nuclear technology for improving the global energy scenario. India must target nuclear energy to support at least a 10 percent share of energy mix for the nation within the next 15 years. In the same time-frame, if renewable technologies contribute another 20 percent share, along with 20 percent from hydropower, cumulatively this could ensure energy independence of about 50 percent by 2030. This would represent a major achievement, both in terms of energy security as well as for contributing significantly towards limiting the impact of climate change.

India must also be proactive in the international efforts towards mitigating the effects of climate change, through positive participation in international dialogue. Although the Kyoto Protocol did not demand any specific targets for developing countries by 2012, perhaps both India and China could take bold and proactive steps to commit to specific GHG emission reduction targets in the near future, and insist that advanced nations support the cost of changeover to newer clean technologies, as well as invest in renewable technologies, including cooperation in nuclear energy technology.

While the OPEC may want to prolong the heavy dependence on oil by fine tuning the oil price, international groups for environmental protection must build consensus to unite for a coordinated momentum for reducing GHG emissions while increasing potential for clean technologies. It is a unique opportunity for a 'win-win' situation for the global energy scene, which could easily turn in to a 'lose-lose' scenario, if mismanagement and political conflicts are allowed to overtake cooperative efforts. India must play a very proactive role for this global win-win opportunity.

The transport sector may continue to be dependent largely on oil and gas, until other technologies such as electric vehicles and hydrogen fuel-based or compressed air-based engines can mature and compete. In the short term, bio-fuels with lower emission properties can significantly reduce the carbon footprint of the transport sector. Greater use of public transport and use of modern technology such as magneto drive locomotives can result in major savings for the transport sector and CO_2 emissions.

The agriculture sector in India is highly subsidised and a highly energy-intensive field. Existing inefficient pumps can be 30 percent more efficient with retro-fitting of new technologies, and innovative solar pumps can replace thousands of diesel pumps. Action on 10 percent of 15 million pumps can translate to a saving of 4 million electricity units per year. The Green Building Initiative is yet another example where the rapidly growing residential and commercial buildings in cities can be made more energy efficient. Given that the annual energy demand for this sector in India is increasing by 35 percent or by about 5 million kWh per year, green building architecture can provide major benefits.

The Government of India has an incentive scheme, the Green Rating for Integrated Habitat Assessment (GRIHA) where a star rating system is in place for qualifying for financial benefits; a 5-star rating is 50 percent more eco-friendly than a zero star rating of most present buildings. Investments in Green Buildings producing more that 80 percent of its energy needs by on-site renewable energy (solar and wind) generation have an attractive payback period of 4-5 years, with a promise of free electricity for many more years. The future will require many such innovative schemes to reduce the carbon footprint of the building sector.

Policy Priorities and Diplomatic Challenges for India

India's economy is on a fast growth path. It crossed the $ 1 trillion mark in 2009 with expectations of doubling by 2017, and it could perhaps be over $3 trillion by 2030. India's electrical energy needs will be about 510 GW by 2030, which is over three times the 160 GW generated in 2010.[11]

Rapid economic growth is bound to increase India's per capita energy consumption and with an increasing urban population, India's total CO_2 emissions can increase alarmingly. At the same time, the effects of global warming will be more severe on countries like India with a high density of population and its economy being dependent on the monsoon. Hence, India faces an urgent challenge of learning to manage the growing demand of energy

with a clear priority of not allowing its carbon footprint to increase significantly. Given the rising tensions about energy and environment, India may not be allowed by the international community to remain energy intensive for long, nor will it be allowed to demand energy equity as argued till now at international forums.

From an energy security perspective, India must first focus on vastly improving its energy efficiency which is pretty low compared to many leading nations. This will be essential to manage the widening gap between demand and supply. Simultaneously, India must quickly increase the share of clean and renewable energy in its energy basket, so that the carbon footprint of the nation does not increase at the same rate as energy consumption goes up. India has the potential to use more of solar and wind energy resources to increase the share of RE (renewable energy) to about 30 percent by 2030. By March 2012, India was the fifth largest producer of wind energy with about 49 GW generation capacity and this is expected to grow to about 222 GW by 2015.[12]

Globally, the share of renewable energy is expected to increase to 30 percent by 2030 and 50 percent by 2050. By March 2014, India achieved 12.9 percent of its renewable energy potential, totalling 28.8 percent (including hydro-power) of overall installed capacity. Thus India is on track to do even better than world trends.[13]

The potential for solar and wind power is very large—enough to avoid dependence on imported oil and coal and even help reduce the share of nuclear energy, which has its own disadvantages. The National Solar Mission target is 20 GW generation by 2022 but the industry feels that the actual target can be many times more with the right set of incentives from the government. India gets an average of 7 KW of solar radiation energy per sq-metre for over 1500 hrs each year (300 days × 5 hours). Solar Photovoltaic (SPV) technology with the current efficiency of 14-15 percent can thus generate about 1500 kWh per sq-metre each year. Solar energy represents a staggering opportunity for India with increasing efficiency and lowering costs, but mind-sets must change to understand the potential and capitalise the opportunity.

Technology advances with Concentrated Photovoltaic (CPV) systems and Concentrated Solar Thermal Power (CSP) can offer higher efficiency up to 28-30 percent in the near future. However, major investment, political will and time will be required for India to harness this technology. As per 2011 estimates the capital cost per 1 MW generation in India was about Rs. 10 crore for solar, 9 crore for nuclear, 6 crore for wind and about 4 crore for coal

thermal power. But by 2014 the solar cost came down to about Rs. 7 crore per MW. It is no wonder that India revised its solar generation target to 100 GW from the earlier 22 GW.[14]

For a country like India with a large rural population, coal, firewood and biomass will continue to play a major role in the rural energy sector for the foreseeable future. Hence, clean coal technology must be pursued for sustaining the use of coal without increasing the level of CO_2 emissions. Similarly, biomass or bio-fuel, though not totally clean, can be made much less polluting through innovative techniques like efficient micro-turbines and can meet the large demand of rural India that may constitute 25 percent of the national energy demand in the near future. For all renewable solutions, the culture of distributed generation must grow for use of energy close to where it is produced. This would avoid T&D losses of the grid and improve efficiency. India must pursue all possible avenues to tap new, clean and sustainable energy resources.

India is a partner in the International Thermonuclear Experimental Reactor (ITER) Project that aims to produce commercial electrical energy from a controlled thermo-nuclear fusion reactor using sea water derivatives to give almost unlimited power from a non-radioactive reactor. Technical feasibility has been already proven. Commercial viability is yet to be achieved.

According to recent estimates by the OECD, unless urgent corrective steps are taken, global GHG emissions could rise by 50 percent by 2050 (one and half times the 2012 level) with irreversible consequences, hence, serious climate action must begin soon. The Conference of the Parties, COP 17 at Durban in November-December 2011 left it to individual nations until 2015 to decide on signing binding commitments for mitigation actions, to be effective by 2020. This could clearly be 'too little too late' because due to cumulative increase in GHG concentration our earth may be already very close to crossing the safety limit of 2°C rise.

Human civilization has to stem the increase of GHG emissions within the next 5-6 years regardless of the increasing energy demands on account of economic progress or increasing population. In order to prevent a runaway situation in future, global GHG emissions must begin to reduce drastically by 2020 and come down to 1990 levels, well before 2050. This will require the present generation to change their lifestyles for serious commitment to energy conservation and increasing energy efficiency. At the same time, there must be concerted global efforts for moving towards sustainable and clean energy resources such as solar, wind and other renewable energy sources. This

presents the only win-win option, rather an opportunity and this must be done for the sake of the next generation otherwise humanity can be on the brink of disaster.

The challenge for India is unique because while it must provide electricity to millions of deprived people, it must also address the energy demands of a growing economy. However, India is now under close watch by other nations to ensure that India's carbon footprint does not grow alarmingly. Indian diplomats at international forums have to ensure that India's priorities do not get compromised due to external pressure. For this, they not only need to have facts and figures on their fingertips, but also an adequate understanding of technological nuances to know the limits to negotiations. India is unlucky that the global economic slow-down is affecting its own development agenda and it is in this environment that India also needs urgent and heavy investments for aggressively promoting renewable energy (RE) options as also R&D for future technology options.

Climate Change and National Security: Indian Perspective

Concerns for India's National Security Interests

The world today is getting increasingly globalised and interdependent with the very definition of national security changing from protecting geographic national borders from enemy forces—to a broader concept of comprehensive security that includes safe-guarding diverse issues of national interests. This may start with basic human security and go on to include internal 'homeland' security, economic security, energy security, water-food security and of course the military security comprising strategic assets, missile defence, outer space assets and cyber security. Hence, the basic safety, stability and capacity for competitive performance of modern society have become integral components of national security, and it is this basic foundation of a secure and stable nation that can come under serious stress due to the adverse effect of climate change.

Despite a growing understanding of the long-term security implications of climate change, the subject has generated more debate in international forums rather than any concrete collective steps being taken to mitigate the effects. Now with the imminent threat to global peace and security due to the possible extreme effects of climate change, there is growing international focus on the potential common dangers of climate change and hence, there is an emerging urgency for collective action to limit its adverse effects. Given

that poorer developing countries will be affected more severely, the subject is of great importance to India's national security.

India is particularly vulnerable to climate change because of heavy dependence on both the monsoon precipitation pattern and glacial sources of water reserves in the Himalayas. Scarcity of fresh water resources in the region will intensify the inter-State and intra-State disputes over territories that either have water resources or control the flow of water to other territories. For instance, the Indus and its tributaries flow through Jammu and Kashmir (J&K) into Pakistan-occupied Kashmir (PoK) and parts of Pakistan. The importance of J&K for India thus needs to be appreciated in this context also. The Baglihar Dam has been a matter of dispute between India and Pakistan, and given the various intra-State water disputes within Pakistan's Punjab-Sindh-Baluchistan regions, scarcity of water is bound to add more intensity to existing conflicts.

The Indus Water Treaty that allows India to build hydro-electric plants on the rivers flowing into Pakistan, without affecting the downstream water flow, could easily fall victim to any new water crisis. Climate change can thus trigger a new level of conflict between India and Pakistan. Similarly, China's plans to divert the flow of the 'Brahmaputra' river to suit Chinese interests, has already created tensions in India. China's continued exploitation of Tibetan resources also has serious long-term implications for India's water resources and the effects of climate change will aggravate the situation.[15]

Concerns about global warming are beginning to be taken seriously all over the world, and the Nobel Committee recognised the cause to be important enough for the IPCC to deserve the peace prize in 2007 for their in-depth study of global warming. Modern society has caused significant changes in the global ecosystem balance and set-in processes that can pose grave threats to human security in future.

Throughout history, the earth has experienced oscillations between warm and cool periods. The shifts in climate can be attributed to a variety of natural factors that include orbital variations, solar fluctuations, volcanic activity and the atmosphere's concentration of GHG. The balance in the earth's ecosystem has been maintained by virtue of the planet's own natural greenhouse effect of trapping heat in the atmosphere to balance the cooling of the earth. However, the changes observed today are occurring at a more rapid rate than is explainable by known natural cycles. Nature's balance is getting affected by human activity on a scale that is too fast for nature to compensate and recover,

posing a possible runaway danger of global dimension. This can be a serious security threat to large sections of the world's population.

Since climate change is a slow phenomenon it has not attracted the kind of attention accorded to weapons of mass destruction (WMD) or the asymmetric threat of terrorism. However, the cumulative consequences of undesired climate changes could be more devastating than the clear and visible dangers of the present time. History has on record many conflicts and wars over control of critical resources and the negative effects of climate change on natural resources are undeniable. Effects of climate change can increase stress among societies combined with fierce competition for scarce resources, conditions that can lead to unprecedented tensions and dangers to stability and security of modern societies.

Since these climatic processes, beyond a point, cannot be stopped or reversed by human intervention, the effects of climate change could easily snowball into dangers to national security, in a sense more dangerous than potential threats from WMD or international terrorism.[16] The linkages between economic security, resource availability and climate change are complex but quite substantive. However, since these dangers are not so imminent, the implications of climate change for national security have been often underestimated. Clearer appreciation of climate change and its impact on the national security interests of individual nations has begun only recently, and will certainly deserve more attention in the future.

For India, large-scale migration from coastal areas due to a rise in sea levels and loss of cultivable land is a more immediate concern. Climate refugees from neighbouring Maldives or Bangladesh will add a new dimension. Mass migration from Bangladesh that seems to be sinking deeper into Islamic extremism can create serious problems for societal stability and internal security in India. India has its own share of water-related disputes between states such as Tamil Nadu with Karnataka, Punjab with Rajasthan and Haryana etc. The effects of climate change can aggravate these disputes. The coastal areas of the Sundarbans and other parts will face the same problems as Bangladesh, causing the population to move to safer lands and cities. Economic disparities and inequitable distribution of resources can create new levels of tension when stress levels are already high. The effects of climate change in India can thus very easily lead to social unrest and anarchy beyond the control of government agencies. Unfortunately, such situations are ideal for the rise of militancy and anti-social activities—a serious threat to human security.

The impact of climate change on the military's efficiency can be serious. Extreme weather conditions can cause stress to the military personnel and impact military operations by affecting weapons systems, platforms, bases etc. In extreme environmental conditions cost of maintenance of operating equipment increases considerably and the service life of equipment is reduced dramatically. In future, climate change—whether hotter, drier, or wetter—will add stress to weapons systems as well as personnel. More storms and rougher seas increase transit times, contribute to equipment fatigue and hamper flight operations. Severe weather will have a direct effect on military readiness and efficiency, as experienced in the Thar desert in Rajasthan during summer months. Ships and aircraft operations are made more difficult during heavy rains or storms. Military personnel themselves must evacuate or seek shelter under extreme conditions. As extreme weather events become more common, so do the threats to national electricity supply grids and other supply lines for fuel, food and water. All these create logistic problems for military efficiency and thus increase vulnerabilities if under threat of war. The adverse effects of climate change during peacetime can get even more devastating during wartime and thus seriously impair the efficiency of forces in border areas and in combat situations.[17]

Based on existing data, it appears that the effects of climate changes in the next few decades could pose serious threats to global peace and security. The predicted effects of climate change over the coming decades include extreme weather events, frequent droughts and flooding, retreating glaciers, rise in sea levels, loss of agricultural land, habitat shifts and the potential increase in the spread of life-threatening diseases. In the national and international security context, climate change threatens to add new hostile and stress factors which have the potential to create frequent natural disasters on a scale far beyond what has been seen in the past. The consequences could very likely create political instability where societal demands exceed resource availability and create situations beyond the capacity of local governments to cope. Given the nature of the modern globalised world that is more interdependent and more aware than ever before, scarcity and inequitable access to basic resources like water, food and shelter will be a recipe for escalating tensions and chaos, that can pose a distinct threat to stability and security at all levels—societal, national as well as international.

Unlike most traditional national security threats where the threat is perceived from an identifiable enemy acting in threatening ways over a specific timeframe, climate change has the potential to result in less visible but more

complex situations where interdependent conditions, occurring locally or globally within the same timeframe, can pose serious threats to national stability and global security. The consequences could further erode economic and environmental conditions as food production declines, clean water becomes increasingly scarce, diseases increase and large populations begin to migrate in search of livelihood and safety, besides causing stress and conflict between nations. Such situations can easily lead to an increase in internal conflicts, fractured societies and act as an incubator of civil strife, genocide and growth of extremism and terrorism. Climate change can thus act as a threat multiplier for instability, particularly in the volatile regions of the world and seriously exacerbate already marginal living standards in many developing nations. Concepts of security today are very closely linked to stability and order within the nation.

Climate change presents a new and very different type of national security challenge. As global warming causes the average temperatures to rise, different regions would face varying impacts of temperature change, combined with the fear of the unknown in future. This is likely to create extreme tensions between nations and between different regions. It is the impact of temperature increase on natural systems including habitats, precipitation patterns, extreme weather events, ice cover, sea level etc. that will have serious implications for national security. Human civilizations have grown and flourished over the last five millennia, mainly because the world's climate has been relatively stable. But the global surface temperature has increased by 0.8°C since the beginning of the 20th century and studies suggest that the earth is getting warmer now at a faster rate than it has ever been in past 5000 years. If climate changes significantly and environmental conditions deteriorate to irreversible levels, societies can become highly stressed, human security can be seriously compromised, regional tensions could rapidly escalate and nations or even regions could become unstable, leading to international conflicts and possible war situations.

The nature and pace of climate change being observed today and the consequences projected by the consensus in scientific opinions, are fairly serious and pose grave implications for the national security perceptions of most nations. Moving beyond the arguments of cause and effect, it is important that security analysts across the world should join the environmentalists and begin to address these potentially devastating effects of climate change on national security. The increasing risks from runaway climate change need to be addressed immediately because they will almost

certainly get worse if one delays corrective action. Climate change, energy security and national security are a related set of global challenges and because the issues are closely linked, solutions to one would affect the other.

Geo-Strategic Implications of Climate Change

The future effects of climate change will stem from a more unstable process, involving sudden and possibly, in some cases, catastrophic changes. It is possible that the effects will be felt more rapidly and widely than anticipated, leading for example, to an unexpected increase in extreme weather events, challenging the collective and individual capacity to respond. The stress that climate change will put on our national security will be different than any that one has dealt with in the past. Unlike the security challenges that we are used to dealing with, the effects of climate change will manifest very slowly and silently but very certainly and they will affect every nation, simultaneously but perhaps with varying degrees. The developed world will be far better equipped to deal with the effects of climate change, while some of the poorest regions may be less equipped and get affected more. Climate change may thus aggravate the economic divide between societies/nations and contribute to conditions that can fuel extremist ideologies and anti-rich sentiments.

Many developing countries do not have a strong government and social infrastructure to cope with the types of stresses that could be brought about by global climate change and when a government can no longer deliver services to its people, ensure domestic order, and protect the nation's borders, conditions are ripe for turmoil, extremism and terrorism to fill the vacuum. This is one major effect of climate change that has now caught the imagination of Western developed nations, while in fact it is the poorer developing nations that will fall prey to such conditions first, and face grave threats to their national security. Such stresses can not only lower the threshold of conflict but also threaten the fight to end poverty in developing countries.

Much of Southern Asia and particularly India is predominantly agriculture-based where the health of the monsoon season determines the economic trends and even political stability. Water issues therefore are very important, because adequate supplies of water for drinking, irrigation, and sanitation are the most basic prerequisite for human habitation. Changes in rainfall, snowfall, snowmelt and glacial melt have significant effects on fresh water supplies and climate change is likely to seriously jeopardise all of these factors. A modest rise in temperature of about 2°C in mountainous regions can dramatically alter the precipitation mix by increasing the share falling as

rain, while decreasing the share falling as snow. The result can cause more flooding during the rainy season, a shrinking snow/ice mass and less melting of snow to feed rivers during the dry season. In India, nearly 80 percent of water is used for agriculture and untimely snow-melt is a serious concern as water from the summer melt of mountain glaciers is reducing rapidly, with the glaciers shrinking fast. Major rivers in India originate in the Himalayas and if the massive snow/ice sheet in the Himalayas—the third-largest ice sheet in the world—continues to melt, it will dramatically reduce water supply to most of Asia. There are predictions by reputed institutions which have undertaken simulation projects, that by 2050, large parts of India and China will face severe scarcity of water.[18]

Access to vital resources, primarily food and water, can be a major causative factor of conflicts, a number of which are already playing out today in Africa, like in Darfur, which provides a case study of how existing marginal situations can get acute beyond the tipping point, by climate-related factors. It also shows how lack of essential resources threatens not only individuals and their communities but also the region and the international community at large. Crop ecologists estimate that for every 1°C rise in temperature above historical norms, grain production will drop by 10 percent. Most of the world's growth in food and water demand is occurring on the Indian subcontinent and in sub-Saharan Africa—areas that are already facing acute shortages. Over the coming decades, these areas are expected to become hotter and drier as a consequence of global warming and the situation can become very stressful.

Land loss and flooding will cause displacement of major populations. About two-thirds of the world's population lives near coastlines where critically important facilities and infrastructure, such as transportation routes, industrial facilities, port facilities, and energy production and distribution facilities are usually located. Any significant rise in mean sea level would mean potential loss of land and displacement of large numbers of people. Rising sea levels will also make coastal areas more vulnerable to flooding and land loss through erosion. Storm surges will take a greater toll on coastal communities and infrastructure as sea levels rise. Most of the major rivers and river deltas in the world are densely populated along their banks. As sea levels rise and storm surges increase, saline water can contaminate groundwater, inundate river deltas and valleys, and destroy croplands. This will cause major movement of populations to inner land and cities, away from the coast. This very much represents the likely scene for India in near future.

Although climate change may initially force migration of people due to

economic hardship, the larger concern will be movement of asylum seekers and climate refugees who due to ecological devastation become settlers in others' areas. Any such mass migration will add to global tensions. Over the next few decades, sea level rise could potentially cause displacement of tens of millions of people from low-lying areas such as Bangladesh, Maldives and Sri Lanka. Such migration can lead to international political conflict. Already we have large-scale migration from Bangladesh to India, mainly due to economic reasons. Political turmoil in the region is already a cause of concern.

Most climate projections indicate increasing monsoon variability, resulting in increase in both flood and drought intensity in temperate and tropical Asia. Sea level rise, water scarcity affecting agricultural productivity and increased spread of infectious diseases are the primary climate-induced effects expected to cause problems in Asia. Climate change is expected to increase the geographic range of vector borne diseases such as malaria, dengue fever etc. Climate projections indicate that the Asia-Pacific region as a whole is likely to become warmer and wetter in the coming decades, creating conditions conducive for disease to spread, with certain regions becoming more prone to epidemics.

To live in stability, human societies need access to certain necessary resources, the most important of which are water, food, shelter and health support. Any loss or mismanagement of these basic necessities can undercut the stability of local populations and affect regions on a national or international scale. Disputes over basic resources may not automatically trigger violent outcomes but things can change when situations become more acute. In areas with strong governments and societal cohesiveness, environmental concerns could in fact foster greater cooperation between neighbours. However, if mismanaged, the same situations could lead to increased tensions and conflict. This is what progressive nations must realise and take proactive steps to create the framework for international cooperation on common dangers such as climate change.

Most astronauts confirm how beautiful the earth looks from space with its thin atmospheric layer that shines against the sun light and how utterly vulnerable it appears in the larger scheme of things. The realisation that this protective atmosphere of the earth is getting eroded due to over-consumption by human societies for development and security is frightening. Several astronauts who were exposed to this larger perspective from space are thus becoming environmentalists.

Now with serious security implications of climate change becoming more real, it is time for security forces and defence planners to analyse how best the military can be a catalyst for mitigating environmental threats and global warming. National security consequences of climate change should be fully integrated into national security planning and national defence strategies. Defence forces should enhance operational capability under challenging climate conditions by adoption of improved processes and innovative technologies that result in improved military efficiency. Weather forecasting techniques must be modernised to vastly improve the capacity to monitor patterns of climate change and also develop reliable early warning systems for extreme weather conditions for the country. Some advanced countries are known to be already working on the possibility of using weather as a weapon in the future, although for now it is only at a simulation exercise level. However, the potential of climate change as a threat to security needs to be recognised in all its dimensions and factored into national security planning.

Water and Food Security for India: Impact of Climate Change

India has 16 percent of the world's population but only 4 percent of the total available freshwater and water resources that vary widely by season and by region, within the country. Per capita water availability in India has fallen by almost 70 percent since 1950. This is due to increase in water usage by all categories of water users and rising demand posed due to economic growth and an increasing population, which not only restricts potential uses of available water but also threatens future use. India's main water resources consist of the annual monsoon rainfall and melting Himalayan glaciers in its river flows. The annual extraction of groundwater in India is one of the highest in the world as it provides for over 60 percent of the irrigated land. The growing dependence on groundwater has considerably lowered water tables and this has had an adverse impact on the quality and quantity of rural drinking water.

While demands for energy and food keep growing as population grows, uncertainties and risks associated with fresh water access are bound to get aggravated under adverse climate changes. Building dams, reservoirs, irrigation channels and flood barriers are indeed important options for addressing water issues, but these are meant to complement nature's own reservoirs, watersheds, wetlands, aquifers and floodplains. However, man-induced climate changes are likely to weaken these natural infrastructures and make water management much more difficult in the future.

India gets an average 1,197 mm of rainfall every year. This amounts to a total precipitation of 4,000 billion cubic metres. However, 3,000 billion cubic metres are lost due to runoffs, and only the remaining 1,000 billion cubic metres are available as surface and ground water sources. Water accessibility differs between different user groups. Access to water is often guided by social status and over 16 percent of the rural population and 4 percent of the urban population still lacks access to drinking water.

Numbers are more alarming with regard to water for sanitation facilities. 46 percent of the urban population and 59 percent of the rural population have no direct access to sanitation facilities. India has only about 200 cubic metres of storage capacity per person.[19] The National Water Mission, which was established under the National Action Plan on Climate Change, aims to tackle this problem by generating 20 percent improvement in storage capacity. The average per capita availability of water, currently estimated at 1,600 cubic metres per year, is expected to fall to around 1,000 cm per year by 2025, based on current population projections. Per capita water availability in India is expected to decline to as little as 1/30th of per capita availability in the United States.

According to the assessment of the IPCC on the vulnerability of India to climate change, key challenges are most likely to be surface warming, rise in sea levels, decreasing water availability due to glacial retreat, significant reduction in crop production and loss of flora and fauna. Climate projections indicate inescapable temperature increase by over 2°C by 2050 and even relatively small climatic changes can have a huge impact on water resources, particularly in arid and semi-arid regions such as northwest India.[20] Glaciers form the main source of water for key perennial rivers such as the Indus, Ganga and Brahmaputra.

Almost 67 percent of the glaciers in the Himalayan mountain ranges have retreated in the past decade and will continue to retreat further, diminishing flow and leading to severe water shortages. The frequency and intensity of extreme weather events such as heat waves, droughts and floods, have increased over the past two decades and will increase further due to climate change. With rising sea surface temperature in the range of 2-4°C, cyclone intensity can increase by 10-20 percent and rising sea levels will lead to salt intrusion into coastal fresh water sources and threaten water availability.

Signs of sea level rise are already there along vast stretches of the Sundarbans, the world's largest mangrove wetland in the Ganges-Brahamputra Delta. Coastal megacities, such as Mumbai, Kolkata and Chennai are suffering

from increased erosion and the loss of coastal protection from ecosystems such as coral reefs and wetlands. Rise in sea water temperature has led to large scale coral bleaching along the Indian coast line.[21] Glacial retreat, decreased rainfall and increased flooding in certain areas will threaten water availability as a result of population growth and climate change.[22]

Adverse impacts on water availability due to a decrease in rainfall in some parts and increased flooding in certain other areas can endanger the economy and food security, as well as the livelihoods of rural communities. Water stress on an unprecedented scale will be the most serious consequence of climate change in India. India is highly vulnerable to climate changes because its large population has a high dependence on climate and water-sensitive sectors such as agriculture and forestry for livelihoods. Any adverse impact on water availability would threaten food security, cause destruction of natural ecosystems, including of species which sustain the livelihoods of rural households, and adversely impact economic growth and energy security. The successful implementation of a national water policy responsive to climate challenges will require both a dependable knowledge base and appropriate institutional support at the national, regional and local levels, as well as the financial resources for implementation of priority schemes.

Temperature and its associated seasonal patterns are critical components of agricultural production systems. Rising temperatures associated with climate change will have a detrimental impact on crop production, livestock, fishery and allied sectors.[23] It is predicted that for every 2°C rise in temperature, the GDP will reduce by 5 percent. Accelerated global warming has already been observed in the period ending 2007, mainly due to accelerated warming between 1998 and 2007. This warming was mainly due to the post-monsoon and winter seasons and the average temperature was measured in 2008 as being 0.82°C over the past hundred years. The pre-monsoon and monsoon temperatures also indicate a trend towards further warming.

Overall in India, the physical impact of climate change would likely be seen as:

(1) An increase in the average surface temperature by 2-4 degrees celsius,
(2) Changes in rainfall pattern during monsoon and non-monsoon months,
(3) A decrease in the number of rainy days by more than 15 days,
(4) An increase in the intensity of rain by 1-4mm/day and
(5) Increase in the frequency and intensity of cyclonic storms.

Indian agriculture is doubly vulnerable as around 60 percent of India's total agricultural areas are rain-fed, and thus highly susceptible to monsoon variations. In addition, more than 80 percent of farmers in India are small and marginal farmers with little capacity to cope with climate change effects on agriculture. Climate change will affect food security through its impacts on all components of global, national and local food production chains. Existing projections indicate that future population and economic growth may require doubling the current food production in India, from 2 billion to 4 billion tons of grains annually. However, agricultural production in many countries including India would be severely compromised by climate variability and increase in frequency and patterns of extreme weather events.

In India, livestock are an integral part of the agricultural system. Often, the cropping pattern is interlinked to availability of fodder for the livestock, forming an important component of food security in India and other South Asian countries. Dealing with climate change would require strengthening the resilience of farmers and rural communities and helping them adapt to the impact of climate change. It is also important to explore strategies to mitigate and adapt to climate change, in several key policy domains such as food security. One must examine suitable mitigation strategies to lower emissions from the agricultural sector. In addition, it is important to explore how adaptation activities can result in mitigation as a co-benefit and also how these measures can be integrated into the overall development approaches and agenda.

Policy makers need to be better informed about the regional impact of climate change on water supplies and on ways of adapting to it. In this context, major efforts are needed to improve the regional accuracy of predictions about how climate change will affect water supplies. This is essential to build policy makers' confidence in predictions at the local level, and convince them to take steps needed to adapt to water shortages or surpluses that their communities may face. Secondly, the technology needed to address these concerns should be adaptable for taking local conditions and capacities into account. Communities will only adopt new strategies if they are convinced that they would work, if they have both the knowledge and the means to put these strategies into effect.

The anticipated impacts of climate change pose additional stress on food production systems under pressure to satisfy the food needs of a rapidly growing and progressively wealthier world. As agriculture develops and becomes more intensive in its use of land and water resources, its impact on

natural ecosystems becomes more and more apparent. Damaging the integrity of these ecosystems undermines the food-producing systems that they support. The assessment of viable and effective adaptations to the impact of climate change on water and agriculture will require a sound understanding and integration of agronomic science with water management and hydrology. Due regard for the resulting environmental interactions and trade-offs will be essential.

As the global population heads towards more than nine billion people by 2050 (under medium growth projections), the world is rapidly becoming urbanised and wealthier. Food preferences are changing to reflect this with declining trends in the consumption of staple carbohydrates, and an increase in demand for luxury products—milk, meat, fruits and vegetables—that are heavily dependent on irrigation in many parts of the world. Future global food demand is expected to increase by about 70 percent by 2050, but it will approximately double for developing countries. All other things being equal (that is a world without climate change), the amount of water drawn by irrigated agriculture will need to increase by 11 percent to match the demand for biomass production.

In response to global warming, the hydrological cycle is expected to accelerate as rise in temperature increases the rate of evaporation from land and sea. Thus, rainfall is predicted to rise in the tropics and higher latitudes, but decrease in the already dry semi-arid to arid mid-latitudes and in the interior of large continents. Water-scarce areas of the world will generally become drier and hotter. Both rainfall and temperatures are predicted to become more variable, with a consequent higher incidence of droughts and floods, sometimes in the same place. Agriculture will also be impacted by more active storm systems, especially in the tropics, where cyclone activity is likely to intensify in line with increasing ocean temperatures. Evidence for this intuitive conclusion is starting to emerge. Sea level rise will affect drainage and water levels in coastal areas, particularly in low-lying deltas and may result in saline intrusion into coastal aquifers and estuaries. Another consequence of greater future water demand and likely reduction in supply is the emerging competition between the environment and agriculture for raw water, and matching of supply and demand will thus become harder to reconcile.

Given that climate change will have far reaching effects on Indian agriculture and food security, it is important that the country prepares itself to adapt to these changes, and does so quickly. Coping with the impact of climate change on agriculture will require careful management of resources

like soil, water and biodiversity. Making agriculture sustainable is imperative and it is possible only through production systems that make the most efficient use of environmental goods and services without damaging these assets. If climate change impacts can be incorporated in the design and implementation of development programmes right away, it will help to reduce vulnerability, stabilise food production and better secure livelihoods. A large-scale climate literacy programme is necessary to prepare farmers, who are today bewildered by the rapid fluctuations in weather conditions that affect agriculture. Their traditional knowledge does not help them to manage these recent anthropogenic changes. By 2050 about half of India's prime wheat production area could get heat-stressed, with the cultivation window getting shorter, affecting productivity. For each 1°C rise in mean temperature, wheat yield losses in India are likely to be around 6 million tons per year, or around $1.3 billion at current prices.[24]

Climate Negotiations: Challenges for Indian Diplomacy

Status of International Cooperation

In 1988, the United Nations Environment Programme (UNEP) and the World Meteorological Organisation (WMO) established the IPCC to synthesise all climate change-related research and provide a scientific review of the current state of climate knowledge. The first IPCC assessment report, published in 1990, inspired the international community to develop an international political platform to coordinate their response to the issue. The United Nations Framework Convention on Climate Change (UNFCCC) was subsequently developed to provide such a platform.

The UNFCCC held several discussions between February 1991 and May 1992 to address the need for joint action to combat climate change. The Convention was opened for signature during the United Nations Conference on Environment and Development (UNCED) at Rio (hence called the Rio/ Earth Summit) in June 1992. The UNFCCC entered into force on March 21, 1994, shortly after the 50th instrument for approval (known as ratification) had been received. To date, 195 countries have ratified the convention. These countries are referred to as the "Parties" to the convention.

The ultimate aim of the Convention is to stabilise GHG concentrations in the atmosphere at a level that will prevent dangerous human interference with the climate system. The Convention also provides that such a level [of GHG concentrations] should be achieved within a time-frame sufficient to

allow ecosystems to adapt naturally to climate change, to ensure that food production is not threatened, and to enable economic development to proceed in a sustainable manner. In order to attain this objective, the convention provides for the creation of various bodies, especially the 'supreme body' of the Conference of the Parties (COP). The COP is an association of all the countries that are Parties to the Convention.

The COP is assisted by two subsidiary bodies. The Subsidiary Body for Scientific and Technological Advice (SBSTA) links scientific, technical and technological assessments, the information provided by competent international bodies, and the policy-oriented needs of the COP. The Subsidiary Body for Implementation (SBI) was created to develop recommendations to assist the COP in reviewing and assessing implementation of the Convention and in preparing and implementing its decisions. Parties realised that in order to address the actions that drive climate change, concrete commitments were required from participating countries, and this led to the negotiation of a protocol beginning in 1995.

The Kyoto Protocol was adopted in Kyoto, Japan, on December 11, 1997. It commits industrialised countries to stabilise GHG, according to the levels agreed to in the Protocol, instead of simply encouraging them to do so. This agreement represented the first time that binding emission reduction targets were set for 37 industrialised countries. During the years 2008-2012, the 37 countries were to reduce their GHG emissions by an average of 5 percent compared with their GHG emission levels in 1990. The Kyoto Protocol focused more on developed countries, because there was recognition that they were to be held 'historically responsible' for the increase in GHG. Developing countries were not bound by specific emission reduction targets through the Kyoto Protocol. Developed countries, as well as countries in transition to a market economy, are known as Annex I Parties under the UNFCCC. In order to enter into force, the Protocol needed ratification by at least 55 parties, and those parties needed to account for at least 55 percent of global CO_2 emissions in 1990. This threshold was reached at the end of 2004, and the Protocol became a legally-binding instrument on February 16, 2005. But the US remained outside the Kyoto Protocol.

During the period between the adoption of the Kyoto Protocol and its entry into force, the Buenos Aires Plan of Action, which was agreed to in November 1998 at the fourth meeting of the Conference of the Parties (COP 4), defined the process for finalising the rules and operational details of the Protocol. At COP 7 in Marrakesh, Morocco, in November 2001,

delegates reached agreement on outstanding matters with the signing of the Marrakesh Accords. These Accords consisted of a package of draft decisions on many of the details of the Kyoto Protocol, including the flexible mechanisms, reporting and methodologies, land use, land-use change and forestry (LULUCF), and compliance. The Marrakesh Accords also addressed issues such as capacity building, technology transfer, responding to the adverse effects of climate change and the establishment of three funds, namely the Least Developed Countries Fund (LDCF), Special Climate Change Fund (SCCF), and the Adaptation Fund (AF).

Since the Kyoto Protocol entered into force, countries that signed the agreement and observing countries have gathered each year during the COP meetings for formal discussions on implementing the Protocol, in what is called the Meeting of the Parties (MOP) to the Kyoto Protocol. In December 2005, at COP 11 in Montreal, Canada, MOP 1 was convened and delegates began to address the post-2012 period (when the first commitment period in the Kyoto Protocol expired) and established a new subsidiary body as an Ad Hoc Working Group (AWG) on Further Commitments. Delegates established a 'Dialogue on Long-term Cooperative Action to Address Climate Change' by enhancing implementation of the Convention. Both the Dialogue and the AWG aimed to address potential future climate change agreements.

Two years later, at the UN Climate Change Conference at Bali in December 2007, delegates adopted a roadmap to initiate a new negotiating process. The Bali Action Plan aimed at long-term cooperative action beyond 2012, and devising strategies for implementation on five issues: (a) shared vision (b) mitigation (c) adaptation (d) technology and (e) financing. The goal was to finish these negotiations in time for the 2009 Copenhagen Climate Change Conference, so that a successor agreement to the Kyoto Protocol could enter into force by the end of the first commitment period in 2012. Approximately 120 heads of State and government attended the UN Climate Change Conference in Copenhagen, Denmark, in December 2009, but this high profile event, was marked by disputes over transparency and process. During the high-level segment, informal negotiations among the heads of State and government from many of the major industrialised countries and representatives of regional and other negotiating groups resulted in a political agreement called the Copenhagen Accord. This was then presented to the COP plenary for adoption. After 13 hours of debate, delegates ultimately agreed to "take note" of the Copenhagen Accord, which meant it was not legally binding.[25]

The Copenhagen Accord called on parties to the UNFCCC to identify their country's priorities for taking mitigating actions. In 2010, over 140 countries indicated support for the Accord, and more than 80 countries also provided information on their national mitigation targets or actions. However, no agreement was reached on long-term goals beyond 2012. Therefore, parties agreed to extend the mandates of the Ad Hoc Working Group on Long-Term Cooperative Action (AWG-LCA) and Ad Hoc Working Group on Further Commitments for Annex I Parties under the Kyoto Protocol (AWG-KP) for another year. In 2010, in Cancun, Mexico, the COP adopted the Cancun Agreements, which included key steps forward in mitigation, adaptation, transparency of actions, technology development, mobilisation of finance, actions to protect forests, and building capacity globally. Parties recognised the need for deep cuts in global emissions in order to limit global average temperature rise to 2°C and to keep the global long-term goal under regular review.

At Durban, South Africa, in November-December 2011, parties to the Kyoto Protocol agreed on a second commitment period of the Protocol to begin in 2013. Delegates agreed that a new agreement with legal force involving the efforts of all countries under the convention would be finalised by 2015, and enter into force by 2020. Parties also agreed to launch the new Durban Platform for Enhanced Action (ADP) with a mandate 'to develop a protocol, a legal instrument or an agreed outcome with legal force under the Convention applicable to all Parties.' The new negotiating process, which began in May 2012, is scheduled to end by 2015. The outcome is expected to lead to firm commitments—Intended Nationally Determined Commitments (INDC) from individual countries for implementation actions commencing from 2020 onwards.

Developing countries generally work through a coalition called the Group of 77 to establish common negotiating positions. This Group originally had 77 members, but has now expanded to include approximately 130 members. China usually cooperates with this group, so it is often referred to as the Group of 77 and China (G-77+China). The Alliance of Small Island States (AOSIS) consists of 43 low-lying and Small Island Developing States (SIDS), most of which are also members of the G-77, and are particularly vulnerable to sea-level rise.

Analysis of the 2050 Scenario: World Beyond 2°C

According to broad scientific consensus today, stabilising atmospheric CO_2 concentrations below 450 ppm, will give the world a 50 percent probability

of limiting warming to 2°C above pre-industrial levels. The 2°C target was formally agreed at COP 15 at Copenhagen 2009. Governments agreed to launch a review in 2013 to consider strengthening the long-term goal of remaining under the 2°C benchmark.

Since 2000, the rate of decarbonisation has averaged 0.8 percent globally, a fraction of the required reduction. Because of this slow start, global carbon intensity now needs to be cut by an average of 5.1 percent a year from now to 2050. It is unrealistic to expect that decarbonisation could be stepped up immediately—which means that the reduction required in future years is likely to be much greater than 5.1 percent. Whilst the international negotiators continue to focus on a 2°C scenario, many climate experts are now worrying about more pessimistic scenarios for global temperatures in the range of 4°C and 6°C.[26]

The pace of reducing global carbon intensity has been slow, despite the growing international focus on climate change. The financial crisis, which started in 2008, dampened progress even further—carbon intensity has fallen by less than 1 percent between 2008 and 2012. In the year 2010, major European Union economies managed the highest rate of decarbonisation, with the United Kingdom (UK), Germany and France all reducing carbon intensity by over 6 percent in 2010-2011. Both UK and France also witnessed increased generation of low emission nuclear power, whereas Germany's exit from nuclear power generation is reflected by its relatively lesser decline in emissions. Emissions in the US fell by 1.9 percent in 2011. A mild winter helped, but the shift from coal towards gas in its fuel mix and more efficient vehicles on the road may help decarbonisation in future.

Australia is a region where climate change is projected to cause more frequent and extreme weather. Since 2000, Australia averaged 1.7 percent reduction in carbon intensity, on par with other developed countries. But carbon intensity grew significantly in 2011 (6.7 percent), reversing the decarbonisation seen in 2010. Heavy rainfall in Australia in early 2011 boosted hydropower generation but it also disrupted mining operations in Queensland and impacted the level of coal stocks at power stations. A return to normalcy saw Australia's carbon intensity increase correspondingly. This is an indication that carbon intensity and performance is often guided more by local conditions than by a firm commitment to protect the environment.

In China and India, the reduction in carbon intensity seen in the last decade appears to have stalled. In both countries, strong GDP growth was closely coupled with rapid emission growth, despite commitments at Durban

to significantly reduce carbon intensity by 2020, relative to 2005 levels (40-45 percent for China and 20-25 percent for India respectively). Meanwhile, Indonesia managed to keep energy emissions broadly stable as its economy grew, with the resulting energy-related carbon intensity falling by 5.2 percent in 2011. Emissions from deforestation and land use change, which account for a large proportion of Indonesia's emissions, have grown significantly in the last few years.

With the inclusion of traditional biomass in overall energy considerations, heating and cooking will remain the principal uses of such renewable fuels over the next 25 years. The power sector, however, is expected to lead the global increase in renewable energy consumption. This sector accounted for a quarter of global renewable energy consumption in 2002, but its share is projected to rise to 38 percent by 2030. Renewable energy, including traditional biomass, accounts for a greater proportion of total energy supplies in developing countries than in developed countries. About 75 percent of renewable energy is consumed in developing countries where most renewable energy production is based on traditional biomass and hydropower. Currently, less than 1 percent of fuels used for transport are renewable. This share could rise to 3 percent over the next 25 years. The overall impact of such changes in developing countries on global energy consumption would be relatively small, although the negative impact of deforestation may be considerable. Industrialised countries account for 23 percent of the total renewable energy consumed worldwide, and transition economies for 3 percent.

While it is common to measure carbon emissions at the source, it is important to remember that it is consumption that drives emissions and indeed, many of the other sustainability challenges of the modern world. Many developed countries are increasingly outsourcing their manufacturing needs abroad to reduce carbon signature. The emission levels of those emerging economies that provide a manufacturing base for the rest of the world would need to be adjusted suitably, if exports were fully accounted for. In the period leading up to the Copenhagen UN Summit on Climate Change in 2009, major economies came forward and pledged carbon reduction targets for 2020. Analyses of those pledges suggest that they are collectively insufficient to meet a 2°C environmental target. With only five years to go, it is questionable whether several of these pledges can be met by 2020, given the scale of the challenge for some of the largest developed economies. In some respects, the economic downturn may make these absolute pledges less challenging. Yet, at the same time, economic pressures may make it much harder to finance the necessary transition towards a low carbon economy.

The challenge isn't necessarily easier for emerging economies either. Pledges to reduce carbon intensity mean curbing emissions at the same time as promoting rapid economic growth. China and India are expected to nearly double the size of their economies by the end of the decade, but emissions must level off soon for them to meet their targets. The majority of any new energy demands will have to be met from renewable energy sources like wind or solar, or even nuclear but not fossil fuel generation, unless it can be compensated with effective Carbon Capture and Storage (CCS) techniques. Russia and Brazil expect slower economic growth, but their emission pledges imply a more drastic cut in carbon intensity than either China or India.

Technology Options and the Way Forward

Delaying effective response to climate change may be politically easier in the short term, but it will entail higher overall costs and more frequent disruptions to normal life in the future. Furthermore, the longer we wait to act upon reducing GHG emissions proactively, greater will be the risk of irreversible adverse change, and harder it will be to reduce emission levels thereafter. To keep the threatening dynamics of climate change within the scope of human control, there is an urgent need to reduce the increasing concentration of CO_2 and other GHG emissions in the atmosphere. Drastic reductions of global GHG emissions will need to be rapidly implemented in order to combat global climate change and its negative consequences.

To stabilise GHG emissions, numerous technologies and/or lifestyle changes can make a big difference. Such strategies include enhancing energy efficiency, increasing the usage of public transport, shifting from carbon intensive sources of energy to carbon neutral sources of energy including nuclear energy, developing carbon capture and storage techniques and increasing the contribution of renewable energy sources such as solar, wind, hydroelectric and geothermal. Clean energy from controlled thermonuclear reactors could indeed emerge as a game changer in the future, but making such fusion reactors available in countries where needed, could perhaps take decades.

All renewable energies are ideal for sustainable development which must become the *mantra* for the future so that development and environment need not be against each other. However, investments in R&D will be necessary to make renewable energy competitive with fossil fuels, for the social transformation needed for the major shift to a green way of life. If crude oil prices go way beyond $ 150 per barrel, interest and investments in renewable

technologies will automatically be high, but if recent efforts in tapping shale oil and gas through fracking seabeds can manage to keep oil prices to acceptable levels, progress on renewable options may see a downturn. The environmental penalty of the fracking process is not known, although it is certain to have adverse environmental effects. And through all the dynamics of international trade, the global carbon signature must reduce rapidly across the world, to slow down global warming so as to remain within a 2°C rise in the temperature of the atmosphere.

Technologies already exist today to support the economic and environmental priorities of individual nations. What is needed is the foresight to balance today's needs with the ecological imperatives of tomorrow. The potential consequences of climate change are so significant that it is vital to appreciate how climate change trends may potentially impact national security, and what actions must be initiated to prevent major destabilising consequences of climate change. In the context of national security, stability is an important precondition to comprehensive security. Maintaining stability within and among nations is often the primary means of avoiding serious conflicts that can lead to wars. Conversely, instability in key areas can threaten national, regional or international security and that is the main threat that uncontrolled climate change presents. International diplomacy will have to face a whole new set of challenges related to climate change and will need to be well informed with latest knowledge.

It is important to acknowledge that technological development need not be seen as independent from people and should be understood as a socio-technical approach in which technological development and human development are influencing one another and creating opportunities for cooperation. Hence, for adaptation to global warming, technology solutions will play a vital role in combating negative consequences. However, the role of social solutions should not be ignored and substituted in favour of technological solutions to achieve sustainability and address global climate change. Society already possesses the mitigation technologies to bring about substantial emission reductions necessary to freeze CO_2 and GHG emissions in the immediate future and work for a sustainable future in coming decades. What is needed is collective resolve to address the problem before the problem overtakes us.

Fortunately, there is increasing recognition of the role of cooperation in the application of S&T for worldwide mitigation efforts. Scientific knowledge and technological innovation is a learning process that is largely achieved

through cooperative or collaborative efforts of sharing experiences, information, infrastructure and other resources. In the emerging new world of complex dynamics between human kind and environment, technology is influencing large parts of our everyday life and it is also cutting across all national boundaries. A paradigm change is in making among societies and nations which demands that competition and cooperation must coexist in the interest of global peace and stability.

More than ever before, S&T is opening new opportunities as well as new concerns for the entire world, albeit at varying levels. On one hand, this may increase the gap between the Haves and the Have-Nots, but on the other hand it is helping evolve a new recognition that for global threats and common good, all mankind must unite for the global cause. Addressing climate change is one such issue that should bring the world together through the realisation that in the context of nature we are all equal partners. Despite competition for economic progress and differences in security perceptions about each other, all nations and societies must come together for preserving the environment.

Climate change needs to be viewed in the context of national security implications and not merely as a matter of social hardship or economic cost. The likely adverse changes in rainfall patterns, fresh water scarcities, increased flooding, sea level rise, spread of diseases etc., pose serious risks to social harmony and political stability world over, and particularly more so for India, which in turn cannot alone solve the problems. Problems due to the vast diversity and increasing gap between the rich and poor in the country can get easily aggravated further by climate change induced stress. Poor infrastructure, corrupt practices and poor governance renders the threat of climate change even graver, since it is not seen as imminent or urgent and hence, does not get the attention it deserves. It is in this context, that climate change must be appropriately linked to national security and foreign policy so that it gets due priority in the planning process of the nation and in international negotiations for sustainable development, energy security and mitigation of global warming.

Climate change is a global problem but there are large differences in emissions of GHG between countries. The patterns of emissions in the past will be different from those in the future. Developing countries are much more vulnerable than industrialised countries due to their greater dependence on agriculture, limited infrastructure, lack of knowledge and technology and due to their limited financial, institutional and governance capabilities.

The main causes for GHG emissions are: increasing population, economic growth imperatives, excessive land use and opportunistic choice of technology

that are intricately linked to development. The development patterns of the present industrialised countries have caused most of the current change in the climate, but its future change will be largely determined by the development patterns of the currently less industrialised countries, which are on a fast growth curve. The UNFCCC contains a number of key notions and principles that are providing guidance on how to handle the distribution of emission reduction efforts. It makes reference to sustainable development, equity and common but differentiated responsibilities and respective capabilities.

The most substantive principles in distribution of mitigation efforts must consider (a) Responsibility: mitigation efforts should be proportional to the contribution to the problem (b) Capability: mitigation efforts should be proportional to the capability to contribute, i.e. depend on income, technology, institutions and natural resources (c) Need: mitigation efforts or emission ceilings should leave room to eradicate poverty and attain a reasonable standard of living or, in other words, should respect the equal right of humans to develop and progress.

In international negotiations over the control of climate change, the developing countries have so far played a limited role. In the Kyoto Agreement on limiting GHG emissions, only a subset of the world's economies, the so-called Annex I countries, have agreed to treaty-based limits on GHG emissions. These Annex I countries are essentially the highly developed economies plus Russia, Ukraine, and parts of Eastern Europe. Developing countries enter the treaty obliquely, mainly through the clean development mechanism, which aims to foster projects linking the developed and developing countries in emission control.

The US is calling for a more active role for the developing world, including binding commitments of GHG by several of the large developing countries. In general, the developing world has resisted such entreaties, arguing that their highest priority is to grow and that growth requires increased emissions of GHG. They stress that per capita GHG in the advanced economies are several times those of the poorer countries, so limiting the emissions of the poorer countries would be unfair.

Climate change is going to affect all nations and hence, it deserves cooperation by all nations, rich or poor, to build a coordinated global response and action. Multilateral cooperation among the leading economies—the US, the European Union, Russia, China, Japan, India and Brazil, could provide the political alliance necessary to achieve drastic cuts in GHG emissions. The

investments required for energy conservation and alternative energy technology are very large and the advanced nations should take a lead in providing support to such efforts in developing countries. However, the industrial countries, having enjoyed the benefits of cheaper resources are reluctant to accept the larger responsibility towards slowing down global warming.

It is estimated that the world economy now needs to reduce its carbon intensity by 5.1 percent every year, till 2050, to have a fair chance of limiting global warming to 2°C above pre-industrial levels. Even to have a reasonable prospect of getting to a 4°C scenario would imply nearly quadrupling the current rate of decarbonisation. The decarbonisation rate required for a 2°C world has not been achieved in any single year since World War II. The closest the world came to that rate of decarbonisation was during the severe recessions of the late 1970s, early 1980s (4.9 percent in 1981) and the late 1990s (4.2 percent in 1999). The expected reduction in emissions resulting from the current economic slowdown has not materialised, partly because of sustained growth in emerging markets.

The observed relationship between economic growth and CO_2 emissions is also asymmetric. Emissions tend to grow proportionally with economic growth, but fall by less than the rate of economic decline. Regardless of the outcomes at the UN Climate Change Summits, one thing is clear—governments and businesses can no longer assume that a 2°C warming world is the worst scenario. The reality could be much worse. The world has already gone past that and any investment in long-term assets or infrastructure, particularly in coastal or low-lying regions, needs to be based on more pessimistic scenarios. Sectors dependent on food, water, energy or ecosystem services need to scrutinise the resilience and viability of their supply chains. More carbon intensive sectors need to anticipate more invasive regulation and the possibility of stranded assets.

The only way to avoid the pessimistic scenarios will be radical transformations in the ways the global economy currently functions. This suggests a need for a much more ambitious climate policy and more urgent action—both at the national as well as international level. These are going to be the monumental challenges for the economists, technologists and diplomats of the future.

NOTES

1. David Spratt and Philip Sutton, "Climate Code Red: The Case for Emergency Action", *Friends of the Earth Report*, 2008, at http://www.ecocivilization.info/sitebuildercontent/sitebuilderfiles/climatecodered.pdf (Accessed May 28, 2014).

2. Jeff Sachs, "Solving the crisis in the Drylands", January 15, 2008, at http://economistsview.typepad.com/economistsview/2008/01/jeff-sachs-solv.html (Accessed May 28, 2014).
3. Will Steffen, et. al., "The Anthropocene: conceptual and historical perspective", *Philosophical Transactions A*, January 31, 2011, at rsta.royalsocietypublishing.org/content/369/1938/842 (Accessed May 28, 2014).
4. "Climate Change: Evidence, Impacts, and Choices", National Research Council of the National Academies 2012, at http://www.nap.edu/catalog/14673/climate-change-evidence-impacts-and-choices-pdf-booklet (Accessed May 28, 2014).
5. R.K. Pachauri, A. Reisinger (Eds.), "Climate Change 2007: Synthesis Report", A Report of the Inter-governmental Panel on Climate Change, Geneva, 2007, at www.ipcc.ch/publications_and_data/ar4/syr/en/contents.html (Accessed May 28, 2014).
6. "Six Degrees Could Change the World", National Geographic Channel, Documentary, 2007, at http://natgeotv.com/asia/six-degrees, (Accessed May 28, 2014).
7. Kurt M. Campbell et. al., "The Age of Consequences: The Foreign Policy and National Security Implications of Global Climate Change", November 2007, at http://csis.org/files/media/csis/pubs/071105_ageofconsequences.pdf, (Accessed May 28, 2014).
8. List of Countries' Energy use per capita, October 20, 2012, at http://www.economicshelp.org/blog/5988/economics/list-of-countries-energy-use- per-capita/ (Accessed May 28, 2014).
9. *Stern Review: Economics of Climate Change*, at http://mudancasclimaticas.cptec. inpe.br/~rmclima/pdfs/destaques/sternreviewreportcomplete.pdf. (Accessed May 28, 2014).
10. Country Share of CO_2 Emissions, Union of Concerned Scientists, 2011 Data, at http://www.ucsusa.org/global_warming/science_and_impacts/science/each-countrys-share-of-co2.html#. (Accessed May 28, 2014).
11. Meeting India's Energy Requirements in 2030, July 2013, at http://www.futuredirections.org.au/publications/indian-ocean/1118-meeting-india-s- energy- requirements-in-2030-1.html. (Accessed May 2014).
12. *Energy Statistics 2014*, Central Statistics Office GOI, Table 2.5, at http://mospi.nic.in/Mospi_New/upload/Energy_stats_2015_26mar15.pdf (Accessed May 28, 2014).
13. "India achieves 12.95% of renewable energy potential", *Business Standard*, June 2014, at http://www.business-standard.com/article/economy-policy/india-achieves-12-95-of-renewable-energy-potential-114060501140_1.html (Accessed Sept 27 2014).
14. "India Officially Ramps Up Solar Power Target To 100 GW By 2022", June 22, 2015, at http://cleantechnica.com/2015/06/22/india-officially-ramps-solar-power-target-100-gw-2022/ (Accessed July 2015).
15. Brahma Chellaney, "Climate Change and Security in Southern Asia: Understanding the National Security Implications", *RUSI Journal*, April 2007, Vol. 152, No.2, at http://chellaney.net/2007/04/16/the-challenge-of-climate-change-in-southern-asia-part-ii (Accessed May 28, 2014).
16. Steve Almasy, "John Kerry: Climate change as big a threat as terrorism, poverty, WMDs", CNN, February 17, 2014, at http:// edition.cnn.com/2014/02/16/politics/Kerry-climate (Accessed May 29, 2014).
17. Halvard Buhaug et.al., "Implications of Climate Change for Armed Conflict", February 25, 2008, at http://siteresources.worldbank.org/INTRANETSOCIALDEVELOPMENT/Resources/SDCCWorkingPaper_Conflict.pdf (Accessed May 29, 2014).
18. Supriya Kumar, "The Looming Threat of Water Scarcity", Worldwatch Institute, March 19, 2013, at http://www.worldwatch.org/looming-threat-water-scarcity-0 (Accessed May 29, 2014).

19. Aarti Kelkar-Khambete, "The sanitation crisis in India—An urgent need to look beyond toilet provision", at http://www.indiawaterportal.org/articles/sanitation-crisis-india-urgent-need-look-beyond-toilet-provision (Accessed May 29, 2014).
20. Ashvin K. Gosain, "Climate Change Impacts on Water Resources in India", at http://www.teriin.org/events/docs/wb_confer/73ashwin_gosian.pdf (Accessed May 29, 2014).
21. Aadi Vaidya et.al., "Effects of Global Warming on the Coasts", at https://www.google.co.in/?gfe_rd=cr&ei=0W8kVoXpEZLnugSPiqvwAQ#q=effects+of+global+warming+on+the+indian+coasts (Accessed May 29, 2014).
22. "Measuring Glacier Change in the Himalayas", UNEP Global Environmental Alert Service, September 2012, at http://na.unep.net/geas/getUNEPPageWithArticleIDScript. php?article_id=91 (Accessed May 29, 2014).
23. Anna Ranuzzi and Richa Srivastava, "Impact of Climate Change on Agriculture and Food Security", ICRIER Policy Series No. 16, May 2012, at http://www.icrier.org/pdf/Policy_Series_No_16.pdf (Accessed May 29, 2014).
24. M.S. Swaminathan, "Green Economy and Sustainable Food Security" October 3, 2011, at http://www.uncsd2012.org/content/documents/Plenary3%20Day1%20M%20S%20Swaminathan%20Whole.pdf (Accessed May 29, 2014).
25. Government of Canada, Canada's Action on Climate Change, "Copenhagen Accord" October 31, 2013, at www.climatechange.gc.ca/default.asp?lang=En&n=AA3F6868-1 (Accessed May 29, 2014).
26. Brad Plumer, "Two degrees", April 22, 2014, at http:// www.vox.com/2014/4/22/5551004/two-degrees (Accessed 29 May 2014).

PART III

Technology and Foreign Policy: Indian Priorities

7

Summary and Recommendations

Technology and Foreign Policy Interplay: A Summary

Our world today is increasingly defined by scientific advancement and technological innovation. Many countries including the US and China view economic competitiveness, national security and the well-being of their population as inextricably linked to their capabilities in science, technology and innovation. Solutions to most of the national challenges today, rely on developments in science and technology (S&T), be it for national security, economic growth, human development or energy and water security issues. Science and technology is now a high-priority endeavour of all nations and even poor developing countries are investing heavily in building S&T core competence for rapid enhancement in national power. Universal reach of technology has made our world much more inter-connected and inter-dependent than ever before and instant information access has changed the benchmark of almost all interactions between societies and nations. International Relations (I.R.) have entered a new paradigm and technology has become the most valuable tool in this new 'Information Age'.

As S&T capabilities are growing around the world, scientists and technologists are conducting research and innovation in a globally connected community and diplomats are also far more engaged with issues of S&T. As a result, the interplay between science, technology and foreign policy has become more synergistic than ever before. Foreign policy today depends significantly upon a country's ability to integrate current scientific and

technological knowledge into diplomacy for projecting 'Comprehensive National Power' (CNP) in international affairs. Science diplomacy requires enhanced linkages between the S&T community, foreign policy makers and diplomatic practitioners to ensure that external policies are technically sound, programmatically viable and politically feasible. The tools to achieve this may be same as before, but the sensitivity and response required is going to be different in different situations or at different times and this will demand an integrated approach towards managing international affairs. This is the fundamental change that international relations of the future will have to contend with and that is the central message that this book has attempted to articulate throughout. India is on a steep curve of emerging as a major world class power and hence, it will need to combine its S&T strengths with foreign policy foresight to work together for an aggressive projection of India on the world stage.

Perceptions of national security have transformed in the past few decades and these now include several priority areas of national interest that go beyond protecting national borders and sovereignty. While strategic planning, military preparedness and self-reliance in defence technology will always continue to be very important, other equally important areas of high concern now include internal security, economic growth, energy security, as well as water and food security etc. On one hand, information security, cyber security and security in outer space represent new dimensions of supreme national security interests while on the other, poverty reduction, quality education, job creation, good governance, curbing corruption etc. define national interests in terms of systemic efficiency and governance. If one were to look for a common denominator for all of the above areas, it becomes very clear that S&T knowledge, technological self-reliance, a culture of innovation and overall techno-economic superiority represent the core of CNP. As modern technology continues to empower individuals with amazing capabilities—both good and bad, it is getting increasingly clear that it is the quality of people that will make nations great in future, and it is the quality of education and awareness that will drive this human quality enhancement, aided by S&T based knowledge, innovation, communication and human desire for development and progress.

India's economic reforms of the early 1990s and its announcement of being a Nuclear Weapon State in 1998, were defining actions of the 20th century that positioned India on the global stage, as a world class power for the new century. The unraveling of the Indian information technology (IT)

potential followed soon thereafter, as well as the grudging recognition of India as a nuclear power. The US forging civil nuclear cooperation in 2005, within seven years after 1998, was quite a phenomenal success of India's foreign policy and technology maturity. The US move was unprecedented, because it was a move that risked weakening the Nuclear Non-Proliferation Treaty (NPT) and India was perceived important enough to take that risk. On one hand, India's impeccable record of responsible behavior with sensitive technology of Weapons of Mass Destruction (WMD) opened-up international cooperation and on the other, India's considerable soft power image—'Incredible India' and its vibrant democracy, peace loving culture, respect for knowledge and non-aggressive national projections—all of this contributed to the rise of India as an important international player.

Despite India's new-found image and its clear aspiration for a great power identity, there has been a gap in how India perceives itself and how others see it. In the absence of a 'Grand National Strategy', Indian policy makers have been found struggling to define how to use this leverage, since there is no clear consensus concerning the nature and scope of the Indian national interest. Hence, despite innumerable pockets of excellence and widespread talent and huge demographic advantage, India has yet to consolidate all the potentials for a robust CNP that should make it one of the three most powerful nations in the world.

India's biggest weakness has been its inability to exercise regional leadership. Far from articulating a clear and attractive vision for the region, India remains a reactive force to regional situations and lacks the initiative to propose bold projects, for example, creation of a pan-South Asian energy independence initiative or a regional carbon emission management initiative or some such pan-Asian idea. However, much of this can change with the National Democratic Alliance Government in power that appears to be more proactive and articulate. This can offer a good opportunity to establish foresighted integrated policy reforms so that India's S&T strengths can be better leveraged for positioning India in its rightful place among future S&T leaders in the international order. The same techno-economic strength will then gain higher credibility in international affairs to help India rise as a world class power.

Security, Technology and External Policy

Control and access to defence technology as well as other dual-use technologies forms an important facet of foreign policy and national strategy. All through

the cold war decades, the US-led Western alliance denied several technologies to erstwhile Soviet-bloc countries. India too suffered under these technology embargoes. India was further isolated by nuclear technology controls when the Nuclear Suppliers Group (NSG) was formed in response to India's peaceful nuclear explosion (PNE) in 1974.

India's exemplary record in controlling sensitive technologies is now being internationally recognised. It has formally established its own technology controls through the SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) list of controls and the Indian WMD Act formulated for enabling India to commence bilateral dialogues to promote dual-use technology cooperation. India is now a partner in several global efforts towards technology management and is no longer perceived as a target for technology denials. This has been an important transition in the context of the interplay of technology in I.R.

Responsible ownership of technology is now emerging as the litmus test for technology cooperation between progressive nations that want to promote technology-use for constructive and peaceful purposes, while preventing its possible misuse. Given the changing international perception of India as an emerging global power and a partner in building global peace, the time is opportune for India to give a major thrust to acquiring erstwhile controlled technologies and equipment for rapid development. India must negotiate with other countries from a position of higher confidence, to extract maximum benefit from technology exchanges. It is here that external policy has an important role to play, in dismantling constraints on technology access and on cost-time factors that overshadow international exchanges. The opportunity must also be used to realise international technology cooperation in critical advanced technologies, as no single country can afford to address the full range and sophistication of the technologies for defence and security.

It should be easy to accept that in the final analysis it is the CNP that would decide the international balance of power equations. It therefore follows, that a country like India cannot aspire to be a global power, without being a regional power in terms of relative techno-economic superiority in the region. India's rapid advance in the Information-Communication-Technology (ICT) sector and its technology maturity as demonstrated in several key areas of progress, has in fact served to bring this recognition of a regional power. Consequently, global perceptions have also changed to recognise India as the only country that can provide a counter-balance to a bullish China in the South Asian region.

Regional power status is dictated by how India's neighbourhood perceives India's capacity, both as a constructive leader, and a world class competitor. Effective diplomacy for projecting national strength is the main tool for influencing perceptions, and technology will be the main enabler in this process, in the future. The factors that can aid diplomacy in moulding perceptions in its neighbourhood are economic progress, indigenous technology base and military superiority. However, much depends on how India's foreign policy and diplomacy can leverage its techno-economic strengths to project India's soft power capabilities, and create desired perceptions in India's neighbourhood and among the larger comity of nations.

While everyone agrees that economic strength will dictate future power equations among nations, there is not enough understanding about the role that technology plays, even in this regard. The following emerging technology trends indicate how external policies and international relations would be dictated by the nation's techno-economic and diplomatic agenda in the immediate future.

- Technological advances in the past few decades have accelerated the globalisation process to create a paradigm change in global security perceptions and techno-military doctrines.
- The most critical technologies for defence are increasingly dual-use in nature with civilian technology advances often feeding military technology requirements.
- Enabling technologies such as advanced computing, micro-miniaturisation, ICT, robotics and artificial intelligence (AI), biotechnology and nanotechnology are transforming the spectrum of defence and security capabilities.
- Advances in sensors, smart materials, missile defence, satellite systems, advanced autonomous systems, energy beam weapons etc. are leading to new capabilities for offence and defence.
- Cyber space and outer space are emerging as the new important domains of the future that will hugely impact every aspect of modern society as well as national security.
- The private sector is increasingly becoming the main player in international technology affairs with the role of government becoming more like that of a facilitator, rather than a controller.
- Diffusion of technology has become an integral component of international transactions. Consequently, preventing misuse of advanced technology is becoming more challenging.

- While technology control will remain important in international relations, new approaches to enable and promote responsible technology cooperation among progressive nations will be vital for future.

For many decades, technology development in India has been need-based and not really driven by any 'Grand National Strategy'. As a result, only the 'need' has been in focus, while technology was perceived only as a tool for intended objectives. There were no long-term plans for synchronising technology development or technology acquisition, with the objectives of foreign policy or diplomatic agenda that are often futuristic. In the international sphere, India therefore, has remained a buyer of technology and not a creator of technology. As a compulsive buyer, India has been getting yesterday's technologies at tomorrow's prices and hence, remained behind most of the developed countries, with consequent diplomatic disadvantages in international relations. But India has the potential to change all that fairly rapidly, and fortunately, the process has already started. This should soon earn India its legitimate power and position in the complex matrix of global affairs.

While there have been many pockets of excellence in India, the nation as a whole still fares rather poorly in S&T in comparison to most other comparable nations. The Department of Science and Technology (DST), Council of Scientific and Industrial Research (CSIR), Indian Space Research Organisation (ISRO), Defence Research and Development Organisation (DRDO) and Atomic Energy Commission (AEC) have been traditionally the five main government departments that have together shaped the S&T scene in the country.

India has however been slow in creating the right ecosystem for rapid growth of technology and innovation, both in the public and private sector to achieve a high degree of self-reliance in high-priority areas. This stagnant environment is now changing, with the private sector playing an increasingly significant role than ever before. For India to really become dominant in technology and innovation there is a need of an innovation ecosystem that links markets, companies, entrepreneurs and research and development (R&D) centres with venture capitalists and financial institutions, for a proactive approach to rapidly catch-up with world technology leaders. This can then enable India to formulate a proactive foreign policy that can quickly position India at the high table, on international issues of high importance in future. As rightly articulated by the new generation of political leadership, India will

need less of government but more of governance to be globally competitive in future.

As is often said, research converts science into knowledge and innovation converts knowledge for wealth creation in society. China is a good case-study of how a well-planned approach to technology development and incremental innovation over two-three decades has enabled the country to compete with the best in the world in economy, technology and military power. India also needs a proactive and aggressive approach to technology planning, development, acquisition and an innovative approach to transform its potential strengths into major capabilities. The process begins with recognising the gaps or the weaknesses in the system and gearing up with an institutionalised approach to leapfrog ahead, with international cooperation wherever possible.

Despite many pockets of excellence, India as a whole still continues to lag behind because of the lack of the desired pan-India ecosystem that must be driven by a coherent and integrated policy. Individual greed and corruption in implementation have reduced the efficacy of even some very good policy decisions in key nation-building endeavours. India needs to very quickly shed this negative image and acquire a reputation as a professional nation. It is abundantly clear that Indian people are eminently capable of being the best professionals in the world as demonstrated by several of them holding leadership positions in the US, Europe and across the world. The same people feel constrained in their own country because of the lack of true meritocracy that alone can foster professionalism.

In the new globalised world, it is the foreign policy and diplomacy of the country that can attract external investments and foster greater cooperation with global partners in nation building, but the process can best succeed when it is supported by well-informed and effective political decision-making. Successful international exchange is ideally a fair give-and-take affair between equal partners that can produce a final win-win result. Thus, the real challenge for India will be to rise rapidly with an integrated national approach that can make India a real equal partner in all important areas of global affairs. The main instruments to achieve this will be technology and diplomacy.

India's National Interests and Foreign Policy Priorities

The foreign policy of a country is framed in a way so as to preserve and promote the national interests in the changing dynamics of international politics. It is an instrument to serve the national security priorities of the

nation, while also projecting national strength at world forums, to best serve national aspirations. On one hand, it needs to be flexible enough to harmonise national interests with regional interests and global concerns; and on the other, it must be routed in clear convictions about certain national priorities that cannot be compromised, no matter what the external compulsions.

India is emerging as a potential world class power with its economy rated as the third largest as of April 2014. India is steadily making its mark in the new world order which is getting more centred on the South Asian region, than the affluent West. It is therefore imperative for India to evolve a consolidated and integrated national strategy which is independent, and is best suited to leverage the hard power of national techno-military capabilities, combined with the soft power of economics, trade, educational and cultural capacities. Indian foreign policy and diplomacy thus, must evolve revised strategies to handle new challenges with new tools and techniques for best projection of the nation in the international arena.

Even as India attempts to catch up with the developed world through faster economic growth, which at present is predominantly fuelled by technology and industrial know-how often imported by Indian or foreign companies in India, the aim is to increase the competitive advantage. Given the mature technical status of the industries and high level of energy consumption, advanced countries have to look for new innovations and new products to remain competitive, even if they have to use 'disruptive' technologies. Some examples of such disruptive technologies of the past can include micro-electronics, personal computers, satellite-based capabilities, mobile phones, automation in manufacturing, and smart materials. India needs to be mindful of these fast developments and orient its priorities suitably, for drawing maximum benefit from advances in technology for the country and its people.

Well before the year 2020, India must put together a national innovation system to lay the foundation for the next phase of acquiring leadership in industries and technologies of dual-use nature. To be able to use external policy as an important element of preserving and protecting national interest, there is need for a more detailed and nuanced understanding of India's economy, the distinctive characteristics of important industries, and how technology choices might play out in the global arena. This would call for a stronger coordination of S&T specialists with diplomatic initiatives. Prudent choices and correct practices will be vital for India to change from being reactive to proactive.

India's diaspora can provide an important channel for tapping global knowledge flows. Non-resident Indians particularly in the US, are well-placed in the technology network, as high level professionals or successful entrepreneurs. They have played a critical role in developing India's IT and business-processing boom. Senior Indian executives in major global corporations have also played an important role in directing investments and outsourced work to India. In addition, many Indian professionals are returning to India to set up global operations. India should focus on such Indian professionals to promote joint research projects and access knowledge networks to support India's national interests.

In the new age of information and communication, the reach of technology has expanded in every field of importance to the nation. It is therefore imperative for bureaucrats and diplomats to recognise the inter-connections between foreign policy, defence strategy and economic agenda and their dependence on the S&T strength or weaknesses of the country. Science and technology is so intrinsic to development and progress in this new age that it will play an indispensible role in determining and influencing the dynamics between nations in times to come. The globalised and inter-dependent world will demand a different approach to international affairs and Indian diplomacy as well as foreign policy must adapt to this new paradigm.

In this context, it is important to review India's foreign policy priorities and align them with changing realities. At the outset, one of the foremost priorities of India's foreign policy is undoubtedly national security. According to strategic analysts, security of the State is attained and preserved through the maximisation of national power and the elements of national strength that can include: geographical size, natural resources, quality of people, internal harmony, strong S&T base and globally competitive economy. All of these contribute to CNP. Foreign policy and defence strategies play an important role in strengthening national image in the neighbourhood and with other nations. Without such an organised and proactive foreign policy, national priorities can get reduced to basic survival parameters.

This is the basic difference between developed countries that enjoy better peace and harmony, as against poorer developing countries that often remain mired in conflicts and regional struggles for survival. Technologies that are critical for defence, security and economic competitiveness provide the superiority needed for deterrence against potential dangers so that a secure nation can focus better on development, progress and peace. India is on the

verge of attaining a developed country status and all national strengths must be combined to achieve this goal at the earliest.

So far, India has been a major buyer of defence equipment from the international market. This was necessary for meeting immediate security concerns during the nation-building phase. But now, as India is emerging as a strong economy and a mature technology player in global affairs, it is important to enhance the national image with core competence in critical technologies that are important to futuristic defence, development and progress. As most important technologies are now dual-use in nature, active participation of the private sector in defence production has become very important for India to become increasingly self-reliant in defence and critical technologies.

Foreign direct investment (FDI) in Indian defence industries, including joint ventures and co-production of defence products is a step in the right direction. FDI in government-approved R&D projects (recently expanded beyond just defence R&D) needs to be incentivised. India's offset policy for defence acquisition has promising possibilities for Indian companies to act as a co-producer and partner, rather than just as a buyer of advanced technology equipment. In all these efforts for rapid progress, defence and diplomacy must join hands to best serve national interests.

Looking at specific security interests, one can easily see the increasing importance of Intelligence, Surveillance and Reconnaissance (ISR) technologies, increasing reliance on autonomous systems as already demonstrated by the impressive performance of Unmanned Aerial Vehicles (UAVs). Similarly, missile defence technologies must compete with advances in attacking missiles, and increasing concerns of security of outer space will demand sharper focus on space relevant technologies, including micro-satellites. Techno-military superiority in these areas and disruptive technologies like energy beam weapons can bring about radical changes to the security perceptions of India, and thus be game changers in the neighbouring region.

The digital age has made electronic dissemination of technological knowledge much more difficult to control. The new focus on internal security/ counter-terrorism has created a range of new dual-use security technologies, where leadership is not limited to any supply cartel. This has shifted emphasis from shielding dual-use technology to a new perspective—to selectively sharing technology information as a strategy for maintaining technological superiority over adversaries, whether on the battlefield or in the market place. This

represents a new paradigm where a country like India, with its sound technology base, can attempt a major catch-up process, to emerge as a serious contender for techno-economic leadership, and thus rightfully claim its position on the UN Security Council.

Fortunately, technology leadership is shifting from the public to the private sector, relying on commercial markets to spur innovation and reduce costs. The security establishment now seems to be adopting a new approach for rapid access to state-of-the-art technology, where civilian efforts often feed military needs. This opens up a whole new set of opportunities for rapid strides in advanced dual-use technologies, to convert India from a technology importer to a future technology exporter.

The most dramatic technology trend of the 21st century is the way ICT is getting integrated and even embedded into most systems of defence and security importance. At the same time, rapid growth of IT-enabled systems and services is exploiting the commercial potential of technology on a global scale. Internet concepts originally developed for military application have created an information revolution in the public domain, and the potential of web-based technologies for commercial applications is yet to be tapped fully. High-speed computing, sensor-integrated intelligent systems, interactive displays, advanced encryption technology and autonomous systems using robotics and AI are some areas where future advances will set new benchmarks for technological sophistication, and introduce new generation dual-use applications. Unfortunately, the same capacity in wrong hands with the evil intention of a single human can have devastating consequences in the future, and can be a nightmare for security practitioners and organisations.

Future security technologists must therefore develop capacities for advanced intelligence-gathering, quick intelligence analysis and accurate situational awareness for supporting quick executive decision-systems. Emphasis must be towards recognising patterns, analysing intentions and predicting motivational gradients. Intelligent Video Surveillance (IVS) technology is one example where explosive growth is happening in the interest of homeland security, as well as for a host of commercial applications. The trends clearly indicate that the emphasis is moving away from traditional military hardware to leveraging information technology for superior situational awareness and swift corrective or retaliatory action with high precision. Preventing these sensitive dual-use technologies from being misused will be the one single most important challenge in the future. Responsible ownership of technology is now emerging as the benchmark for technology transactions

between progressive nations that want to promote technology cooperation while preventing its possible misuse.

Given all that is riding for India in the technology context, the time is opportune for India to give a major thrust to acquire controlled technologies and equipment. India must now negotiate with other countries from a position of mature confidence to extract maximum benefit from technology exchange. It is here that external policy has an important role to play in dismantling constraints on technology access and on cost-time factors that overshadow international exchanges. This maturity can also be used to foster broader international technology cooperation, as no single country will be able to afford addressing the full range and sophistication of these technologies in future.

It is axiomatic that actual technology transfers depend on the domestic technology base. The Indian Government does have a policy of self-reliance in place to boost the indigenous content of defence acquisitions but much greater emphasis is required on long-term defence planning for futuristic and enabling technologies by user services. This will help integrate technology and equipment imports with indigenous development, fabrication and testing. If the latter can be done increasingly by the domestic industry except in highly classified areas, that would contribute handsomely to India's goal of self-reliance in defence preparedness. Hence, opening up the defence sector for the Indian private industries and using the offset policy more aggressively would indeed be the steps in the right direction. Another line of action is to facilitate Indian companies to leverage domestic strengths to perform better in the global markets. For example, Ranbaxy, Dr. Reddy's and other pharmaceutical companies, Bharat Forge, Asian Paints and Aravind Eye Hospitals illustrate some of India's success stories. External policy should support and facilitate such moves not only by big companies but also by small and medium enterprises (SMEs). The global market is not built up just by pure market forces. There are various forms of privileged access as well as targeted denials. Diplomacy has a crucial role to play in solving problems and enabling access to identified technologies on a privileged or commercial basis. A related challenge to external policy is managing restrictive/regulatory trade regimes and Intellectual Property Rights (IPR) issues to enable India to make the technology transition in a rapid and smooth manner.

There are other public good like energy, health, education, water and environment where external policy initiatives should create opportunities for technology upgradation. The International Thermonuclear Experimental Reactor (ITER) project on fusion energy and the US-sponsored Global

Nuclear Energy Partnership (GNEP) are two major international initiatives that have recently inducted India. This is recognition of India's technology maturity and its capacity to contribute to international initiatives. Similar initiatives may be possible in renewable energy, health and education sectors and of course, in mitigating global warming—a major problem for all humanity.

Apart from preparations for forging an international understanding on how to deal with such problems, there are major opportunities for international collaboration in a variety of areas that are science or technology based. Clean coal technologies, carbon sequestration, solar power technologies, power from wastes, small hydro-power technologies, refrigeration technologies, international monitoring of the greenhouse effect and the ozone layer are some areas of energy and environment in which external policies have a critical role, in seeking appropriate external partners for Indian interests.

The subject of alignment of foreign policy with national interest is too vast to be discussed in a single chapter of a book. For instance, there are many areas of cooperation in agriculture, education and the entertainment industry where the Ministry of External Affairs (MEA) can be a catalyst for well-planned collaboration between Indian institutions and suitable overseas players for mutual benefit, and the process itself can enhance India's image in the world. For the sake of keeping focus on national security and national power-related issues, due justice has not been possible on all other issues of national interest in the limited scope of this book.

Soft Power

Another important area of international relations is the use of smart power for best gains for the country. This is a judicious balance of hard power and soft power projections in the international arena. It is crucial in today's knowledge world where a mix of persuasion, coercion and deterrence must be used in I.R. to achieve foreign policy objectives. In contemporary international relations, there is a renewed interest in the potential of soft power in countries like China and India, which were traditionally known for their respective cultural heritage. India has not been very successful in leveraging soft power in its neighbourhood, except for the natural popularity of its Bollywood products. In this context, Indian foreign policy experts need to rework soft power strategies to tap their maximum potential and help India achieve larger goodwill and regional influence, to complement its economic and strategic rise in international affairs. The recent 'Incredible India'

advertisement drive is indeed a step in the right direction to attract tourism—which attempts to build the right image of cultural India.

India has several areas of strength that can be used innovatively for soft power projection, particularly in its neighbourhood. India's strength in ICT and vast population of knowledge workers is a major asset that can help smaller neighbours in their pursuit of economic progress. India can easily become a regional hub for education and skill development in the modern electronic age. India is already emerging as a preferred R&D centre for many multinational technology corporations and structured S&T cooperation can be a major instrument of soft power projection. Cultural exchanges are known for promoting greater regional harmony, while human quality development via yoga and meditation is yet another field where India can become a world class leader. Affordable healthcare for overseas patients and providing medical or nursing education for developing nations can promote unique Indian expertise worldwide.

Cooperation in agricultural advances and water preservation can be very important for addressing regional problems. Likewise, cooperation for energy conservation and greenhouse gas (GHG) emission reduction are going to become very important for mitigating global warming. Regional cooperative strategies for adaptation to unavoidable climate changes and for addressing regional natural calamities are yet another set of environmental initiatives that a country like India must take. All this can add immensely to the soft power of India, but there is no national policy or diplomatic priority given to this vast soft power potential.

The role of S&T in exercising India's soft power can be pivotal if it is well-planned as a policy push. Use of digital technology and the internet for social media interactions is a new powerful tool for public diplomacy. It has opened up enormous potential for a free and transparent mechanism that Indian diplomats should use, for leveraging India's soft power worldwide and some of it is indeed already happening. In 2012, the Indian Embassy in Cairo marked the birth anniversary of Mahatma Gandhi and the anniversary of Arab Spring by hosting a poster contest which in turn was widely publicised via social media, on the topic 'Did you sense the spirit of Gandhi in Tahrir Square?' It drew responses not only from Egypt and India but also from several other African countries, thus, succeeding in integrating the most recognisable Indian icon with the most important political event in the region. The contest was India's way of saluting the Gandhian spirit of the Tahrir Square revolutionaries.

This new public diplomacy tool is a function of changed beliefs of the foreign policy-making elite about the use of new social media in engaging with non-state actors around the globe. In another instance, the Public Diplomacy Division in the Indian MEA used the Twitter network during the evacuation of Indian nationals from Libya in 2011, which demonstrated Indian diplomacy's reformist approach in using digital social network technology for public diplomacy. This is a welcome change and Indian diplomats must be encouraged to use such S&T tools more innovatively in future.

Besides social media, the impact of television (TV) is also very significant, and India could launch an international TV channel to compete with likes of British Broadcasting Corporation (BBC), Cable News Network (CNN) or Al Jazeera. Similarly, establishing bureaus in important capitals around the world would be effective in projecting India's unique social value system and soft power. India continues to have tremendous potential for soft power because of its culture and civilisational links—its large diaspora, popular films, music, art, historical and cultural links with several countries around the world, all contribute to its soft power. A globally inter-connected and digitalised world offers promising opportunities for diffusion of Indian culture to every corner of the world to enhance soft power.

Grass-root innovations for S&T cooperation, leveraging language skills, achieving high competence in IT management and resolving issues of international trade and intellectual property can go a long way in projecting India's soft power as a knowledge economy, as against the common perception that developing or poor countries can at best be 'workshops' of the world.

Another primary focus of Indian foreign policy should be our immediate neighbourhood—particularly the instability emanating from the violence in Pakistan, Afghanistan and Bangladesh. Promoting economic and educational progress in these regions can change the aspirations of the local population, and thereby diminish the grass-root support that terrorism seems to enjoy in those areas. Unfortunately, in the recent past, India's long-time friends—Nepal and Sri Lanka, have voiced their growing disenchantment with India. In this scenario, Indian leadership and foreign policy makers must take every step to ensure peace and development in its neighbourhood. A renewed strategy of confidence building measures should be chalked out to ensure this goal and S&T can be a major vehicle for forging new initiatives.

Confidence Building

The role of S&T in confidence building measures has been indispensible in the past and their role in building goodwill and harmony would be even more crucial in the future. S&T is an important instrument of wielding soft power in the neighbourhood, and technical assistance, technical cooperation and transfer of technology are all components of S&T engagement. Especially in the South Asian Association for Regional Cooperation (SAARC) countries like Sri Lanka, Bangladesh and Afghanistan, Indian technology companies can help in development of infrastructure and industries.

Other S&T initiatives with smaller neighbours can include transfer of technology for setting up of crucial small-scale local industries, making Indian patents preferentially available to SAARC countries at special rates and leveraging the Indian IT strength for setting up systems and processes in these countries. All this can add to image-building. As an emerging regional power, India needs to evolve its own foreign technical assistance policy and institutionalise the process of providing technical and economic aid to countries in the neighbourhood for enhancing Indian influence.

Contributing to global efforts to prevent common dangers such as global warming, climate change, religious fundamentalism and terrorism etc. can also be a major instrument of soft power. Global problems and concerns will require global solutions and hence, these will have essential diplomatic dimensions. Science diplomacy will have to play a crucial role here. Since the primary objective of science diplomacy is to support foreign policy objectives with scientific information and advice, it is but natural that international S&T cooperation can proactively help India position itself as a credible global player. Combination of S&T and diplomacy can thus provide tremendous outreach for the soft power of India. S&T cooperation can also contribute significantly to coalition building and conflict resolution, both vitally important to international relations.

Cyber space has now become the fifth dimension for international exchange. The technological potentials are so vast that it is difficult even for technologists to keep pace with rapid developments, and yet diplomats of the future must understand the scope of this technology, and how it can be used productively for international peace and stability. The issue of cyber security is inherently international, even from the perspective of national interest. Being transnational in nature, cyber crimes can only be tackled with the combined efforts of the international community.

The Indian Government and the private sector need to give cyber security a high priority in their security and risk management plans. It would also be crucial to leverage India's strength in IT to pioneer effective solutions to this global problem. It would be necessary to participate in multilateral discussions on rules of behaviour in cyber space. Undertaking joint projects in cyber security with international leaders such as the US, United Kingdom (UK) and China would further India's case as a proactive global player, and extend India's soft power. The use of IT tools and knowledge systems should be viewed as major assets for India's diplomatic success in future.

Scientific values of rationality, transparency and universality can help to build trust between nations and within nations. Indian foreign policy experts must leverage science diplomacy to the maximum, given India's robust S&T framework and human resource. Hence, for foreign policy experts, S&T offers potentially useful networks and channels of communication that can be used to support wider policy goals and wield considerable influence in the global community. The scientific community often works beyond national boundaries on problems of common interest, so it is well placed to support emerging forms of diplomacy that may require non-traditional alliances of nations.

Fundamentalist and terrorist groups around the globe have become increasingly IT savvy and that is emerging as a major international concern. While India may succeed in containing terrorism to a large extent with social engineering, India should aggressively cooperate with other countries through information-sharing protocols about terror networks, their financing, arms trafficking and cross-border linkages etc. If aligned with wider foreign policy goals, these channels of information exchange can contribute to coalition-building and conflict resolution. Hence, robust international technical cooperation can strengthen all priorities of Indian foreign policy in international affairs.

Comprehensive National Power: Role of Science and Technology

The new evolving notion of CNP gives calibrated high weightage to economic, scientific, technological, military, social, educational and cultural aspects of national power. It is an acknowledgement that military strength alone no longer guarantees a nation's security. Knowledge, power and economic capabilities are equally important, as enumerated by India's former Prime Minister Manmohan Singh at the Combined Commanders Conference in

Delhi in 2005. During the 1960s and 1970s, national power was considered synonymous with military power. Hence, most theorists engaged in research on international relations avoided dealing with the phenomenon of power.

This would explain to a great extent, the superpower status of the erstwhile Soviet Union and its unexpected disintegration under economic duress. Since then, the perception of national power has undergone a change and the Chinese call it CNP. It is essentially the sum-total of core national strengths viewed comprehensively in the international pecking order that often define the balance of power among nations.

Comprehensive National Power refers to the combined overall conditions and strengths of a country in numerous areas. In the current transition period, as the world moves toward multipolarity, military might, albeit important, is no longer the main defining parameter of strength. Instead, elements such as economic competitiveness and S&T advances have become increasingly important in the competition for power and influence in the world. An evaluation of current and future strengths requires the inclusion of a variety of factors such as territory, natural resources, military force, economic power, social conditions, domestic government, foreign policy, and international influence.

CNP is the aggregate of all these factors as Deng Xiaoping stated: "In measuring a country's national power, one must look at it comprehensively and from all sides".[1] While CNP is notable for being an original Chinese political concept with no roots in contemporary Western political theory or pre-20th-century Chinese thinking, it indeed represents the changed reality of the modern globalised world.

CNP can be calculated numerically by combining various quantitative indices to create a single number to represent the measure of power of a nation-state vis-a-vis others. These indices take into account both military factors (hard power) as well as economic and cultural factors (soft power) while S&T plays a major role in both. CNP entails a smooth combination of hard and soft power, which is increasingly known as smart power. CNP envisages examination of a wide range of factors that contribute to attaining national objectives across the economy, natural resources, population skills, military power, information and knowledge, governance etc.

At present, China is the foremost proponent of CNP as a national power enhancing tool and a number of studies have been carried out in the country with quantified focus. As an emerging power, India has the potential to

enhance its CNP through a structured programme which involves the entire spectrum of national power, with a view to achieving our goals. Thus, CNP provides a recognised model for internal as well as external security enhancements, and a detailed examination of the same through introspection and evaluation in the Indian context is highly relevant, as CNP is emerging as the scientific method used for predicting power equations among major nations. Chinese ancient statecraft from the Warring States era focused on how a wise leader made strategy according to the power of the State. CNP is the means by which nations can forecast the future international status hierarchy in a multi-polar world.

Experts in CNP consider S&T to be the guiding force in raising CNP. This is established through Deng's emphasis on the need for scientific and technological research and its advanced application in the military and economic arenas. The fact that CNP is a function of hard power and soft power, and both these dimensions of power have technological superiority as a major component, further establishes the role played by S&T in augmenting the CNP of a country.

The basic principles which underline CNP of a country must include:

- Both material power (concrete factors such as economics, military affairs, etc.), as well as emotive power (intangible factors such as quality of people, efficacy of governance, international relations, political stability etc.) that need to be included in an assessment of CNP.
- CNP is composed not only of actual power, but latent or potential power also has a contributing role. Examples of the latter include the findings of S&T research before being applied and utilised, or natural resources that exist, but are yet to be developed.
- The contents of CNP and the roles of these factors have changed throughout history and will continue to do so in future; therefore, new aspects may be added or dropped when evaluating at different time periods. Today, the rapidly increasing significance of information as a source of power is a new realisation. In the present world, because of the development of new means of communication, different types of information about market trends or political changes can be promptly delivered to various places in the world. Therefore, in international relations the role of information power is growing and can be compared with political and economic factors.
- In times of peace, domestic and foreign economic activities are the

most central and important part of CNP, and in this too the significance of S&T for international competition is growing.

- CNP also depends on the level of societal development and the quality of life of its people that adds to political stability and the international image of the country.
- Military capability is the basic component of studies of CNP, measuring international competitiveness and analysing a comparison of forces; during peace times it also is an important factor in strengthening national defence and safe guarding peace.

There is a general consensus that the US is the nation with the highest CNP. As per some estimates top 10 countries in CNP terms in 2011 were—

> 1. The US 2. China 3. Russia 4. France 5. Germany 6. Japan 7. UK 8. India 9. Brazil 10. Turkey.[2] However by 2015 India is expected to improve its ranking considerably.

CNP is the perceived power of a nation which may deter or discourage an adversary, competitor or challenger to act in a manner that is inimical to the former. In this context, it would be relevant to consider Pakistan's ongoing proxy war against India, where India is unable to exert pressure on Pakistan, to actually stop supporting terrorism against India. The CNP analysis positions India as the third most powerful country through 2020 and beyond and hence, it should clearly enable India to exert much greater influence in its neighbourhood. In spite of the obvious advantage of a higher CNP, India has not been able to deter Pakistan from acting against India's national interests. One of the reasons is support from China that Pakistan has managed to garner. However, the clearer reason for this is that India has not been able to evolve a grand strategy that would bring to bear the full weight of its national power to thwart Pakistan's designs. There is thus an urgent need for having an integrated national strategy to enhance India's CNP and project its national power adequately against a smaller enemy. This calls for introspection by the highest policy making organs of the State on the need for a comprehensive national security strategy.

Analysis of the famous American Cuban crisis against the erstwhile Soviet Union or the recent example of Russia acting against Georgia to safeguard its national interests, would illustrate that relationships and interplay between nations are dictated by power perceptions, and a grand strategy based on leveraging all strengths of a nation for a cause demonstrates diplomatic power play based on the CNP of nations. Clearly, such a 'grand national strategy'

must combine all the indigenous national strengths of economic stability, techno-military superiority and foreign policy expertise to protect supreme national interests.

The 21st century world is vastly different from the 20th century world. World population has increased three times in the last 60-70 years, and India is expected to have the largest youth population by 2050. Global Gross Domestic Product has increased eight times over the last five-six decades, and advancement of technology has been the main driver of this growth. The international system has got globalised and it is abundantly clear that the 21st century will be a knowledge century where hierarchy of nations will most likely be determined by the knowledge they generate, rather than by the nuclear missiles and warheads they possess. India, which is already vying to be the third largest economy, will have the potential to get more powerful and influential in global affairs, provided it does not remain tied down by its internal conflicts and weakness.

There is no disputing that the gravest security challenge India faces is that of 'jihadi' terrorism for which the epicentre is Pakistan. Pakistan has been using terrorism as State policy since it acquired nuclear weapons (NW) with Chinese help. China is continuing with its proxy war against India by supporting the Pakistani design to keep India mired in regional conflicts, so as to contain it from growing into a major regional power. US acquiescence towards Pakistan can be understood in the context of its need for Pakistan's help in its war against terror. Thus, India stands on its own in its fight against terrorism and the real issue for India's national security strategy should be about how best to thwart this major threat with its own national power projection, without having to get mired in armed conflicts, even if it be at a sub-conventional level. This will be the real challenge for India's future diplomacy, and a techno-economic edge based on knowledge power will be the most decisive factor in this strategy.

The way to achieve this would be to have a future world order where India improves its CNP to match the best in the world, which India rightfully deserves. The enhanced CNP itself may then act as an effective deterrent against China-Pakistan designs to keep India bleeding with low intensity conflicts. In the emerging world order, the realistic option for India therefore, may be to have a strategic partnership with the US to ensure that China does not become the foremost knowledge power of the world. This type of re-alignment will also ensure that the future world order will be pluralistic, democratic and secular. In the process, India will have the best chance to

narrow the gap between itself and China. This in itself should be one of the major goals for India's 'grand national strategy'.[3]

Recommendations

For many decades, technology development in India has been need-based and not really driven by any grand national plan linked to its foreign policy, to project India as a powerful and yet peaceful nation. As a result, only the 'needs' have been in focus in a reactive policy posture, while technology has been perceived merely as an instrument for meeting the needs. There were no long-term plans for synchronising technology development or technology acquisition with the objectives of foreign policy or the diplomatic agenda. It is interesting to note that technology denials became the major motivating factor for Indian foreign policy to become involved in India's struggle to gain indigenous technology competence, to be more self-reliant in the competitive world, so that India could exercise its own independent foreign policy priorities.

As already argued, India has emerged as a potential world class power and what India does or does not do, is now closely watched by most other nations. The main challenge for policy experts in the country will be to make India quickly achieve the power status commensurate with its real techno-economic strength and its techno-military prowess. It is therefore imperative for India to recognise the vital linkages between foreign policy, defence strategy, economic agenda and technology agenda of the country to evolve an integrated 'grand national strategy'. Only then India can best leverage the hard-power of techno-military superiority, combined with the soft power of economics-trade-cultural equations, to serve the larger diplomatic or foreign policy objectives of the country.

There is thus need for a comprehensive plan that would not only strengthen India domestically but should also enable India to be at the right place in the international order. In doing so, it will be necessary to achieve integration of key areas of S&T, economics and foreign affairs with national security at the national policy-planning level in a proactive manner, with a clear foresight of India's aims and aspirations in future; for what India needs most is a strong and techno-savvy political leadership that can synchronise India's strengths in technology, diplomacy and economics to build a strong nation that India deserves to be. Some recommendations are suggested here for combining technology and diplomacy to achieve such a long-term goal for the country.

1. The increasing role of technology in international affairs needs to be recognised by foreign policy experts and diplomats who are responsible for protecting national priorities at international forums. Increasing numbers of foreign policy professionals and diplomats should get relevant technology familiarisation through an institutionalised process before being assigned to an international responsibility.

The role of S&T in international affairs in the present 21st century is far more important than ever before and the impact of technology is increasing steadily in modern society. Much of the globalisation processes and the consequent inter-dependency among societies are because of the inter-connections brought about by advances in ICT. Technology has enabled modern civilisation to move towards a knowledge-based society where information flow is instantaneous and situational awareness is much improved. In this changing paradigm it is very important to understand the significance of the S&T dimension of international relations and the changing patterns of future diplomacy among nations.

The forces of globalisation and impressive advances in enabling technologies have dominated the political and corporate agenda that is defining the new paradigm of competition and cooperation, having to co-exist among most progressive nations. Technologies of global reach are changing benchmarks and timelines of the geopolitics of international interactions and diplomatic perceptions. There is increasing realisation of the impact of technology on economic progress, military might as well as statecraft that shapes the balance of power equations among nations. Hence, technology will continue to be one of the most sought-after commodities in international affairs in future.

2. There is urgent need to introduce S&T training and familiarisation of the young diplomatic cadre for nuanced understanding of technologies of high impact to international relations. Similarly, young scientists/ technologists need familiarisation with foreign policy priorities for orienting their efforts towards providing best support to the international agenda of power projection of India.

External affairs training institutes should have special capsules on S&T as relevant to foreign policy priorities, and even include mid-course update training in specific areas of international negotiations where S&T knowledge plays a prominent role, areas such as nuclear proliferation, space security or

climate change. Likewise, S&T professionals should get specific orientation to understand the relevance of their work in international affairs, so that they can complement national diplomatic efforts whenever needed.

Many advanced nations have instituted offices of S&T advisers at their embassies and External Affairs Ministry offices overseas to ensure timely S&T advisory in conduct of diplomatic negotiations. Science diplomacy must support foreign policy objectives with scientific information and advice so that foreign policy objectives can be fine-tuned in keeping with the dynamic changes in international technology parameters. This can in turn facilitate enhanced S&T cooperation and that again in turn would help improve international relations. Combining technology and diplomacy can thus be doubly beneficial.

3. There is a need for synchronisation of national expertise in security analysis, strategic technology planning along with foreign policy and international law.

The concepts of strategic defence and diplomacy have undergone a significant transformation—driven mainly by technology advances and human innovation. Advanced nations routinely use well-structured 'Think Tanks' and support of the academia for strategic analysis and decision-making. Such a culture is imperative for proactive planning but this is lacking in India, due to historical reasons of being under foreign rule for a long period. Such synchronisation of knowledge and experience will be vital for India to evolve a comprehensive national strategy to become more competitive in the modern world.

The nature of interactions among powerful nations is changing rapidly where cooperative security is becoming imperative in many sensitive areas. Professional and nuanced understanding of inter-connected issues including technology, diplomacy and international law will be vital for mature global interactions. India needs to acquire such new abilities of combining diverse expertise available in the country for larger national objectives. Such synchronisation could also enable India to bring out White Papers on strategic policy as a mechanism for projecting national power and influencing international perceptions.

4. There is an urgent need for a special foreign policy focus on outer space and cyber space vulnerabilities. Most foreign policy challenges of the future will be concentrated in these two new domains because of their vital links to strategic affairs.

In the arena of outer space, there is urgent need for international convergence on how best to monitor and regulate the use of outer space for military purposes without creating any arms race in space. Successful science diplomacy and international dialogue will be vital for preventing misuse of space technology that can challenge peaceful access to this Global Commons for all mankind. India being one of the major space-faring nations must address its own priorities in outer space for formulating its own space policy and then articulating the same suitably, for projecting national priorities in outer space, and protecting national security interests.

Cyber space is the new expanding domain where technology and international relations are more intertwined than any other area of international affairs. The issues are very complex and transcend sovereignty of national borders. Hence, India not only needs a very well-informed and sensitive policy-making capability on the subject, but would also need cyber-familiar diplomats to successfully negotiate India's position at world forums. Indigenous cyber technology capability will be very critical in this endeavour and robust R&D and innovation in government as well as in the private sector will be essential for remaining ahead of the competition. International cooperation and domestic multi-agency integration for policy implementation will be crucial to keeping ahead of the adversary in these new domains.

5. There is need for revisiting India's doctrine for nuclear deterrence and missile defence. The revised doctrine must recognise new security realities and changing international dynamics.

Nuclear-missile deterrence has been an important instrument of diplomacy in international affairs. Deterrence dynamics in future may however demand new approaches based on new technologies for higher situational awareness and high precision non-nuclear pre-emptive strikes to contain threats. Technology is thus already providing newer alternatives for deterrence with space-based networked capabilities. The future of deterrence will be a mix of technology and strategy that can decisively deter enemy intentions. CNP will be the key to developing and strengthening diplomatic capabilities for coercion and prevention as and when required.

Traditional nuclear-missile deterrence may continue to be relevant in regional conflicts involving nuclear-capable neighbours; however, effective missile defence technology can make NW rather impotent for deterrence impact. The India-Pakistan nuclear deterrence stability however provides an interesting case study. There are no known weapons ready and targeted against

specific enemy destinations on both sides, and India remains committed to credible minimum deterrence with a no-first-use (NFU) policy.

However, Pakistan seems committed to nuclear first-strike as and when politically deemed fit. It is known to be developing tactical NW with tacit help from China, to lower its NW threshold, so as to get maximum leverage from a minimal nuclear arsenal. India is also vulnerable to dangers of Pakistan's NW/material falling into the hands of extremists who openly declare India, Israel and the US as their prime targets. India's nuclear deterrence would be useless against non-state terrorists.

In a typical war-game scenario, India seems destined to absorb the first nuclear attack or a State-sponsored radiological terrorist attack. India will then be obligated to respond with punitive retaliation that may have to be a counter-value nuclear strike. India may thus be caught in a no-win situation and come out as an aggressor rather than an aggrieved nation. This could invite severe international condemnation and even sanctions that could seriously slow down its efforts to become a major regional power. Pakistan and China would then have the last laugh and India could be left licking its wounds for a long time!

One way out for India to escape this no-win situation is to aggressively negotiate for a nuclear-free zone in its neighbourhood as a first step towards a universal NW free world. This is a goal India has always advocated and a goal that the world seems to want to move towards in the near future. Aggressive articulation of India's strategy on deterrence can help correct international perceptions about India's vulnerability and compulsions. Any diplomatic complacence in this matter can be a costly mistake.

6. Climate change and energy security will require a very focused and consistent external strategy to balance national priorities with global imperatives. A joint national task force consisting of scientists, environmentalists, lawyers and policy experts can be of immense importance to India remaining proactive on the issue.

In the realm of climate change, diplomatic challenges will be at two levels. Firstly, it will be about how best to negotiate for India's growing energy needs and its inevitable impact on carbon emissions. India will have to convince the advanced group of nations to accept that India direly needs to maintain economic growth and cannot take drastic steps to reduce total national carbon emission.

Secondly, it will be about how to achieve an international consensus on a just and equitable distribution of global energy resources and carbon

allowances in the immediate future. The solutions will be intimately connected to how technology of clean and renewable energy can be deployed to limit the global emission of GHG. For future diplomats, this is an immensely challenging area where individual national interests may not be convergent with I.R. compulsions and yet global cooperation will be critical for the survival of the human race in future.

There are many technical nuances to this energy-environment dilemma and international complexities with challenging consequences. Climate change will probably dominate all future international relations much like the nuclear proliferation focus of the past half century. In India, we need to evolve a mature strategic vision that would allow India to take a leadership role because India will perhaps be the first major victim of climate change if the monsoon becomes unpredictable and climate refugees compound India's internal security and threaten national security. Management of climate change will be a huge challenge that will require combining all resources and expertise to support a sound strategy.

7. There is need for a Grand National Strategy for India for rapidly enhancing its CNP to assert itself as a responsible regional power. Only then can India truly achieve a developed nation status and become a global player in preventing future technology misuse and in promoting global peace and harmony.

Technology and economics will be the common denominators of future progress for India. A progressive foreign policy backed with knowledge-based diplomacy can position India as regional power and a major force in international affairs. That should be the 'grand national strategy' for India.

Meaningful international relations in future will be based on commonality of strategic/economic interests and credibility in responsible handling of dual-use technology. Ironically, technology denial was instrumental for India to synchronise foreign policy with S&T needs and the security of the nation. Now astute foreign policy and a well informed, smart diplomacy can help India rise to be a major global player in technology and security affairs.

The real long-term challenge in the future will be to ensure that while enabling technology is shared equitably among nations to reduce the global divide and tensions, sensitive dual-use technologies are not misused to work against the common good of humanity or environment. Responsible ownership of technology will perhaps emerge as the most coveted qualification

for international cooperation in India's march towards global peace and stability.

Given India's record of responsible international behaviour and history of its natural inclination for peace and tolerance, it can perhaps rightfully take a global leadership role in pursuit of global sustainable development and peaceful co-existence.

NOTES

1. Karl Hwang, "New Thinking in Measuring National Power", WISC Second Global International Studies Conference, University of Ljubljana, Slovenia, July 23-26, 2008, German Institute of Global and Area Studies, at http://www.wiscnetwork.org/ljubljana2008/papers/WISC_2008-137.pdf (Accessed June 7, 2014).
2. Anatoly Karlin, Top 10 Powerful Countries in 2011, at http://*akarlin.com/2011/01/top-10-powerful-countries-2011/* (Accessed June 7, 2014).
3. V. Krishnappa and Princy George, *Grand Strategy for India 2020 and Beyond*, Pentagon Security International, 2012, at http://idsa.in/book/GrandStrategyforIndia2020and Beyond.html (Accessed June 7, 2014).

Index

A defence technologist of great distinction, Professor Amitav Mallik has done a pioneering study on the interface between science and technology and diplomacy with focus on the contemporary global scene. He analyses with great precision the development of new weapons systems, advances in space technology and the exponential spread of Information and Communications Technology (ICT) that collectively pose significant challenges to the security and welfare of the world today. The dilemma faced by India is illustrative. India has made impressive strides in science and technology, especially in ICT. And yet, it remains notably vulnerable to the threats of cyber-crime, cyber-terrorism, cyber-espionage and cyber-warfare. India has a long way to go in developing a policy of "space security" in sectors like missile-defence, micro-satellites and directed energy technology. In each of these areas of technological challenges, Amitav Mallik offers valuable and well-timed policy guidance. Writing in a clear and concise language – devoid of technological jargon, the author reassures policy makers that smarter use of new technology can succeed in "reshaping diplomatic agendas to meet old challenges in new ways". This slim volume is a valuable toolbox not only for strategic analysts, but also more relevantly, for practitioners of Indian diplomacy.

Ambassador Lalit Mansingh
former Foreign Secretary of India
former Ambassador to the USA
and former High Commissioner to the UK.

It is today widely recognised that the possession of and capability in advanced technologies is one of the most important drivers in International Relations. Professor Amitav Mallik's timely book on the *Role of Technology in International Affairs* puts the focus on those technologies impacting on a nation's security, pointing out the paradoxes and dilemmas which arise from the very existence of such technologies. He emphasises the power that these technologies give to countries, both to protect their foreign policy objectives through modernisation of weapons systems and through the denial of such desired technologies to countries on which they wish to exert pressure and influence. They are therefore both tools and commodities in International Relations. This is particularly relevant to a country like India which has been the target of such technology denial regimes till recently. The availability of some of these technologies to non-state actors presents a new challenge to which answers are still being sought. The book makes a valuable addition to the understanding of the complex interplay between technology and international affairs in the changing modern world. I am sure many will find the information in this volume of great interest.

Ambassador Arundhati Ghose
former Permanent Representative of India to the United Nations at Geneva

PENTAGON PRESS
www.pentagonpress.in

Rs. 995/-
ISBN 978-81-8274-881-1
9 788182 748811