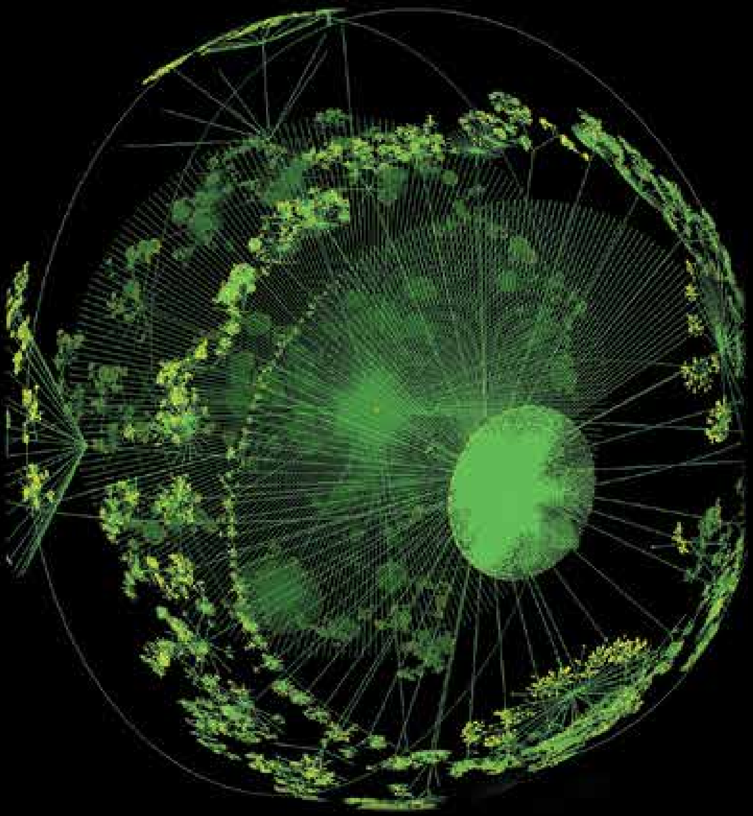
Navigating the Indian Cyberspace Maze

Guide for Policymakers



Ashish Chhibbar

Navigating the Indian Cyberspace Maze

Guide for Policymakers

Navigating the Indian Cyberspace Maze

Guide for Policymakers

Ashish Chhibbar

KNOWLEDGE WORLD

KW Publishers Pvt Ltd
New Delhi

MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

Disclaimer: The views expressed in this book are those of the author(s) and do not necessarily reflect those of the Manohar Parrikar Institute for Defence Studies and Analyses, or the Government of India.

Manohar Parrikar Institute for Defence Studies and Analyses
No. 1, Development Enclave, Delhi Cantt.
New Delhi-110 010
Phone: +91-11-26717983
Website: www.idsa.in

ISBN 978-93-89137-47-7 Hardback

Published in India by Kalpana Shukla

KW Publishers Pvt Ltd
4676/21, First Floor, Ansari Road
Daryaganj, New Delhi 110 002
Phone: +91 11 23263498/43528107
Marketing: kw@kwpub.com
Editorial: production@kwpub.com
Website: www.kwpub.com

Printed and bound in India

The content of this book is the sole expression and opinion of its author(s), and not of the publisher. The publisher in no manner is liable for any opinion or views expressed by the author(s). While best efforts have been made in preparing the book, the publisher makes no representations or warranties of any kind and assumes no liabilities of any kind with respect to the accuracy or completeness of the content and specifically disclaims any implied warranties of merchantability or fitness of use of a particular purpose.

The publisher believes that the contents of this book do not violate any existing copyright/intellectual property of others in any manner whatsoever. However, in case any source has not been duly attributed, the publisher may be notified in writing for necessary action.

Contents

Abbreviations

ACO	Ant Colony Optimiser
AES	Advanced Encryption Standard
AGI	Artificial General Intelligence
AGR	Adjusted Gross Revenue
AH	Authentication Header
AI	Artificial Intelligence
AIM	Analytics India Magazine
AIS	Artificial Immune System
AISHE	All India Survey on Higher Education
ALIS	Autonomic Logistics Infrastructure System
ANN	Artificial Neural networks
APT	Advance Persistent Threat
APT	Asia Pacific Telecommunication
ARP	Address Resolution Protocol
AtoN	Aids to Navigation
BaaS	Blockchain as a Service
BBNL	Bharat Broadband Network Limited
BCH	Bitcoin cash (Crypto currency)
BCO	Bee Colony Optimiser
BFSI	Banking, Financial Services and Insurance
BI	Business Intelligence
BIMSTEC	Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation
BPO	Business Process Outsourcing
BSNL	Bharat Sanchar Nigam Limited
BSV	Bitcoin Satoshi Vision (Crypto currency)
BTC	Bitcoin (Crypto currency)

BTS	Base Transreceiver System
C2W	Command & Control Warfare
CAN	Campus Area Network
CAS	Chinese Academy of Science
CCA	Controller of Certifying Authority
CCMF	Cyber Combat Mission Force
CDMA	Code Division Multiplexing Access
CDS	Clinical Decision Support
CDS	Chief of Defence Staff
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIO	Critical Information Infrastructure Operators
CISO	Chief Information Security Officer
CNMF	Cyber National Mission Force
CNO	Computer Network Operations
CO	Cyberspace Operations
COA	Courses Of Actions
CODE	Collaborative Operations in Denial Environment
COMEST	Commission on the Ethics of Scientific Knowledge and Technology
COP	Common Operating Picture
CPU	Central Processing Unit
CSAIL	Computer Science and Artificial Intelligence laboratory
CSC	Common Service Centres
CSIS	Center for Strategic and International Studies
CSOC	Cyber Security Operation Centre
CSSS	Champion Services Sector Scheme
CTO	Chief Technological Officer
CyPAD	Cyber Prevention, Awareness and Detection
DAE	Department of Atomic Energy
DAG	Directed Acyclic Graphs
DAO	Distributed Autonomous Organisation
DARPA	Defense Advanced Research Projects Agency
DART	Dynamic Analysis and Replanning Tool
DASH	Dash (Crypto currency)

DBT	Direct Benefit Transfer
DCA	Defence Cyber Agency
DCN	Defence Communication Network
DCO	Defensive Cyberspace Operations
DDOS	Distributed Denial of Service
DeitY	Department of Electronics and Information Technology
DES	Data Encryption Standard
DG	Deep Green
DHCP	Dynamic Host Configuration Protocol
DIARA	Defence Information Assurance & Research Agency
DLA	Defense Logistics Agency
DMZ	De-Militarised Zone
DNC	Democratic National Committee
DNS	Domain Name Service
DOD	Department of Defence
DODIN	Department of Defence Information Network
DOF	Degree of Freedom
DOS	Denial of Service
DWDM	Dense Wave Division Multiplexers
EBL	Explanation Based Learning
ELMo	Embedded for language Models
EM	Electro Magnetic
EMI	Electromagnetic Interference
ERCIM	European Research Consortium for Informatics and Mathematics
ESP	Encapsulation Security Payload
ETH	Ethereum (Crypto currency)
EW	Electronic Warfare
FDMA	Frequency Division Multiplexing Access
FIR	First Incident Report
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FLM	Fuzzy logic Model
FTP	File Transfer Protocol
GA	Genetic Algorithms
GAN	Generative Adversarial Networks

GBPS	Giga Bit Per Second
GCI	Global Complex for Innovation
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GFS	Google File System
GGE	Group of Governmental Experts
GIS	Geo-Spatial information System
GLADS	Global Administration Data System
GOI	Government of India
GP	Gram Panchayats
GPR	Government Process Reengineering
GPS	General Positioning System
GVA	Gross Value Added
HADR	Humanitarian Assistance and Disaster Relief
HDFS	Hadoop Distributed File System
HITS	Hyper Link-Induced Topic Search
HMM	Hidden Markov Model
HR	Human Resource
HSPD	Homeland Security Presidential Directive
HTTP	Hyper Text Transfer Protocol
I/O	Input /Output
I4C	Indian Cyber Crime Coordination Centre
IaaS	Infrastructure as a Service
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IARPA	Intelligence Advanced Research Projects Activity
IBW	Intelligence Based Warfare
IC	Integrated Circuit
ICANN	The Internet Cooperation for Assigned Names and Numbers
ICERT	Indian Computer Emergency Response Team
ICMP	Internet Control Message Protocol
ICT	Information Communication Technology
IDS	Integrated Defence Staff
IDSA	Institute for Defence Studies and Analyses
IDSS	Intelligent Decision Support Systems

IE	Information Environment
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IEW	Information Economic Warfare
IGF	Internet Governance Forum
IGMP	Internet Group Management Protocol
IISER	Indian Institute of Science, Education and Research
IIT	Indian Institute of Technology
INEW	Integrated Network and Electronic Warfare
INMARSAT	International Mobile Satellite Organisation
INTELSAT	International Telecommunication Satellite Organisation
INTERPOL	International Criminal Police Organisation
IO	Information Operations
IoT	Internet of Things
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlefield
IPR	Intellectual Property Right
IRC	Information Related Capabilities
IRTF	Internet Research Task Force
ISM	Industrial Scientific & Medical
ISO	International Standards Organisation
ISOC	Internet Society
ISP	Internet Service Providers
ISSC	Information Security Steering Committee
IT	Information Technology
ITeS	Information Technology Enabled Service
ITU	International Telecommunication Union
IW	Information Warfare
IWWN	International Watch and Warning Network
JAIC	Joint AI Centre
JEDI	Joint Enterprise Defence Infrastructure
JTMS	Justification-based Truth Maintenance System
KB	Knowledge Base
KBIL	Knowledge Based Inductive Learning

LAC	Line of Actual Control
LAN	Local Area Network
LASER	Light Amplification by Simulated Emission of Radiation
LEA	Law Enforcement Agencies
LED	Light Emitting Diode
LEO	Low Earth Orbit
LIDAR	Light Detection And Ranging
LoC	Line of Control
LTC	Litecoin (Crypto currency)
MAC	Media Access Control
MAN	Metropolitan Area Network
MARS	Maritime mobile Access and Retrieval System
MBPS	Mega Bits Per Second
MD	Message Digest
MDMP	Military Decision Making Process
MECR	Multilateral Export Control Regime
MeitY	Ministry of Electronics and Information Technology
MFCC	Mel Frequency Cepstral Coefficient
MHA	Ministry of Home Affairs
MHz	Mega Hertz
MIMO	Multiple Input Multiple Output
ML	Machine Learning
MMP	Mission Mode Projects
MMSI	Maritime Mobile Service Identity
MOC&IT	Ministry of Communication & IT
MoD	Ministry of Defence
MOU	Memorandum of Understanding
MSC	Mobile Switching Centre
MTNL	Mahanagar Telephone Nigam Limited
NASSCOM	National Association of Software and Services Companies
NATGRID	National Intelligence Grid
NCCC	National Cyber Coordination Centre
NCFL	National Cyber Forensic laboratory
NCIIPC	National Critical Information Infrastructure Protection Centre

NCSC	National Cyber Security Coordinator
NCSP	National Cyber Security Policy
NCW	Network Centric Warfare
NDCP	National Digital Communication Policy
NDSAP	National Data Sharing and Accessibility Policy
NIC	Network Interface Card
NIC	National Information Centre
NISPG	National Information Security Policy & Guidelines
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NMO	National Military Objectives
NOC	Network Operating Centre
NPA	National Police Agency
NSA	National Security Advisor
NSCS	National Security Council Secretariat
NSPD	National Security Presidential Directive
NTIA	National Telecommunication and Information Administration
NTRO	National Technical Research Organisation
OCO	Offensive Cyberspace Operations
OE	Operational Environment
OEWG	Open Ended Working Group
OFC	Optical Fibre Cable
OFDM	Orthogonal Frequency Division Multiplexing
OGD	Open Government Data
OMB	Office of Management and Budget
OOB	Order of Battle
OS	Operating System
OSI	Open Source Interconnection
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCFG	Probabilistic Context Free Grammar
PCT	Patent Cooperation Treaty
PDDL	Planning Domain Definition language
PDU	Protocol Data Unit

PEAS	Performance, Environment, Actuators and Sensors
PGP	Pretty Good Privacy
PII	Personal Individual Information
PLA	People's Liberation Army
PMS	Preparation of Military Struggle
PoC	Proof of Concept
POFMA	Protection from Online Falsehood and Manipulation Act
PSU	Public Sector Undertaking
PSYOPS	Psychological Operations
QoS	Quality of Service
R&D	Research and Development
RAID	Real time Adversarial Intelligence and Decision making
RARP	Reverse Address Resolution Protocol
RATS	Regional Anti Terror Structure
RBI	Reserve Bank of India
RBL	Relevance Based Learning
RF	Radio Frequency
RJ	Registered Jack
RMA	Revolution in Military Affairs
RNA	Ribonucleic Acid
RSA	Rivest, Shamir and Adleman
SA	Security Association
SA	Simulated Annealing
SaaS	Software as a Service
SAN	Storage Area Network
SAR	Search and Rescue
SCADA	Supervisory Control and Data Acquisition
SCO	Shanghai Cooperation Organisation
SDU	Service Data Unit
SET	Secure Electronic Transaction
SEZ	Special Economic Zones
SHA	Secure Hash Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNL	Space Network List

SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SNS	Space Network Systems
SOP	Standard Operating Procedures
SSL	Secure Socket Layer
STEM	Science, Technology, Engineering and Maths
TA	Target Audience
TAU	Threat Analytics Unit
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiplexing Access
TDSAT	Telecom Disputes Settlement and Appellate Tribunal
TLD	Top Level Domains
TM	Table Manager
TMS	Truth Maintenance Systems
TPS	Transactions Per Second
TRAI	Telecom Regulatory Authority of India
TSP	Travelling Sales Person
UAV	Unmanned Aerial Vehicles
UDP	User Datagram Protocol
UGV	Unmanned Ground Vehicles
UHF	Ultra High Frequency
UHR	Universal Health Record
UIDAI	Unique Identification Authority of India
ULMFiT	Universal Language Model Fine-Tuning for text Classification
UMANG	Unified Mobile Application for New Age Governance
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organisation
UTP	Unshielded Twisted Pair
VLSI	Very Large Scale Integrated
VPN	Virtual Private Network
VSNL	Videsh Sanchar Nigam Limited
W3C	World Wide Web Consortium
WAN	Wide Area Network
WGIG	Working Group on Internet Governance

WIPO	World Intellectual Property Organisation
WMD	Weapons of Mass Destruction
WSIS	World Summit on the Information Society
WTO	World Trade Organisation
XCP	Counterparty (Crypto currency)
XMR	Monero (Crypto currency)
ZEC	ZCash (Crypto currency)

1. Introduction

I dream of a Digital India where cybersecurity becomes an integral part of our National Security.

—Shri Narendra Modi
Hon'ble Prime Minister of India

We are living in an age and time where science fiction is fast turning into reality and everything seems to be possible. Even a couple of years back, it would have been impossible for us to envision a space rocket which after delivering its payload lands safely on a platform and is reused again; or that drones are being used to deliver packages to customers; or fast land transportation systems like Hyperloop, that radically transform the land speed paradigm and are capable of speeds in excess of 1,000 km per hour. Every day, there is news of new discoveries and breakthroughs which have the ability to disrupt multiple segments of our lives and livelihoods ranging from autonomous self-driven automobiles, to autonomous robots and machineries, smart cheap devices which can perform a host of simple as well as complicated tasks, robots that can perform complicated surgeries, to use of Artificial Intelligence to decide on our credit card ratings and loan approvals ...The list is endless.

Most modern day inventions stem from one major achievement – *Digitisation* or the ability to convert words, pictures, signals, voices, videos into a series of electrical or optical impulses that can be manipulated, transported, recreated, retransmitted, stored and again converted back to original word, picture, video – With no/ minimum loss or distortion. Digitisation not only enabled us to convert almost all available text, voice, image and video into a common format of 1s and 0s but also made it extremely easy to store information on common digital storage platforms with life spans in excess of 50 years.

Since, varied information could be digitised and available as a stream of 1s and 0s, the next logical progression of technology was to transport this information from one geographical location to another. This led to the invention of today's internet and as they say – The rest was history. Along with digitisation and transfer of digital information, we witnessed an exponential rise in technology related to digital storage, computation and development of software and applications. Digitisation also led to convergence, or use of a single device to process different formats of digitised information (voice, text, video and imagery) and miniaturisation wherein size and power requirements of storage, computational and transmission systems shrunk, resulting in advent of smart phones and tablets with the storage and computational power in excess of last generational mainframes and super computers.

Cyberspace has turned out to be one of the greatest discoveries of mankind. Today, we have more than four and a half billion people connected to the internet with a penetration rate of 58 per cent. From 2000 to 2019, the internet has expanded at a staggering rate of 1,157 per cent. What is surprising is that people are not the largest users of cyberspace. In fact, against a world population of 7.676 billion, there are more than 26.66 billion smart devices connected to the internet, which generate more data and information than the entire human community as a whole. This number is all set to increase dramatically as the next generation Internet of Things (IoT) devices hits the street and any and all devices ranging from doors, windows, and refrigerators to thermometers and clothes get connected to the internet. Today, we generate roughly 2.5 quintillion (1 followed by 18 0s) bytes of data every day and this figure is also rising at an alarming rate. We regularly double the total data generated till a particular date, in just over next two years.

Thus, as we move along the 21st century, certain broad patterns emerge. First, the pace of development and discovery will increase exponentially. This will result in unimaginable progress and improve the common man's quality of life. Lifespans are bound to increase, most deadly diseases will have a cure, transportation from one place to another will be extremely fast and cheap, manual labour will be a concept of the past, jobs will be few and far between, work timings will drastically reduce and more time would be available for recreation and following one's creative talent and passion. This will be preceded by a period of intense uncertainty, volatility and flux as the human ability to change and adapt will be unable to keep pace with the technology. Second, cyberspace will be all pervasive and essential for day to day survival. Access to the internet will become a universal right. Lastly, technology will be the new currency for power. The technology to manage global cyberspace will become extremely niche and restricted to only a few major mega corporations and nations which would leverage the same to negotiate with other corporations and states.

The cyberspace is currently facing multiple challenges which need to be overcome collectively in shortest possible timeframe to allow the development of a safe, secure, transparent and rule based domain, which is seamlessly available across all corners of the planet and beyond 24×7×365. The first challenge is that currently there are no common rules and norms that govern this important domain. In fact, there is no single acceptable definition of the word "cyberspace". Thus, the absence of global norms and rules encourages criminals and other state as well as non-state actors to use the domain for engaging in illegitimate and illegal activities ranging from selling of drugs, fake currency, IDs and social security numbers to the more sophisticated acts of stealing data, intellectual property thefts, carrying out misinformation campaigns and manipulating democratic election processes. Second, the domain promotes anonymity and plausible non attribution. The present cyberspace allows unhindered access without verification. This results in a domain where fake and multiple names and profiles are a norm and there are sophisticated programmes and applications that remove all traces linking a criminal act to a person, group or nation. Third, the domain is regularly exploited to carry out mass surveillance and violate people's digital privacy. The global nature of operations by multinational companies allows them a level of unhindered access to day to day lives and data of citizens of multiple nationalities. This is coupled by an almost bullying attitude and ignorance of the host country's concerns and laws, as the mega corporations know fully well, that in an enmeshed global environment, the services offered by them cannot be replicated by most host nations. Fourth, technology has reached a stage where we need global understanding and commonality of ethics and morality, which is lacking. Artificial Intelligence (AI) along with advances in new generation devices like the gene editing tool CRISPR, provide us solutions which can have far reaching consequences for the human race. For example, it is now possible to produce designer babies with particular types of build, eye and hair colour, etc. Also AI is capable of producing autonomous lethal weapon systems that can kill and destroy lives and targets without any human interference. Lastly, all the major power centres in the world are converting cyberspace into a domain for warfighting. From a war fighter's view point, cyberspace offers enormous advantages that are rarely offered by natural domains of land, sea, air and space. The impact of cyberspace is global, instantaneous and extremely inexpensive, along with a very high degree of anonymity and non-attributability.

A large number of states have realised the adverse consequences of an unregulated cyberspace and are asserting their right to "cyber sovereignty". This in a broader sense implies subjecting the global mega corporations to greater scrutiny, audit and investigation, local storage of data, blocking access to internet and restricting and filtering content for consumption of people. This kind of cyberspace fragmentation is not really beneficial for the people, state as well as the mega corporations and is a classic example of a lose-lose situation.

India, has been one of the largest beneficiaries of cyberspace. In the mid and late nineties we benefitted from the Y2K problem[1] as Indian software companies and engineers became the saviours of the global computer systems and networks as the world transited into the new millennium from December 31, 1999 to January 1,

2000. Then, the excess bandwidth and capacity of the backhaul Trans National Ocean laid Optical Fibre Cable (OFC) along with an English speaking youthful workforce shifted a majority of Business Process Outsourcing (BPO) projects from USA and Europe to India. Subsequently, we saw an astronomical rise in institutions providing affordable coding skills to a large number of Indians, who migrated to developed countries. They gave rise to a new generation of software developers, who have reached the highest positions of Chief Executive Officer (CEO) and Chief Technological Officer (CTO) of global mega corporations like Google and Microsoft.

The mobile communication revolution witnessed from the late nineties onwards, ensured that India was able to literally leapfrog on the communication front, without going through the tedious transition process from landline to cellular telephony. A visionary leadership was able to foresee the immense advantages of digitisation and mobile communications for the teeming population and ensured that inexpensive mobile phones with affordable unlimited data rates were offered by the telecom industry. This resulted in India becoming the internet hotspot of the world and a major stakeholder in global cyberspace ecosystem, with the highest generation of data and the largest subscriber base of many social media companies like Facebook and YouTube.

The government also leveraged the immense opportunity offered by cyberspace for reaching out directly to the people by cutting out bureaucratic red tape and corruption and improving efficiency. The computerisation of the rail reservation system was the first of many projects initiated by the government, and has immensely benefitted the common man. Thus, it is no surprise that India ranks amongst the leading nations on digital optimism scores, where the citizen feels that technology and connectivity have led to positive and good changes and are the way forward towards prosperity and a better quality of life.

The cyberspace of the future will cover the entire globe and beyond, have an extremely high bandwidth and data rates and would be shaped by three major technologies: AI, Blockchain and Big Data Analytics. As far as cyberspace infrastructure is concerned, 5G technology will offer extremely high speed last mile wireless interconnectivity, which will be utilised for autonomous vehicles, smart cities management, delivery of immersive experiences, etc. OFC is likely to be the preferred choice for backhaul communications till such time as massive satellite Low Earth Orbit (LEO) networks like Star Link of SpaceX do not become a reality.

AI technology has progressed rapidly over the past decade or so and has proved to be one of the leading technologies of the future, owing to the ever increasing generation of data and increase in computational power. The AI revolution has given rise to a number of smart solutions ranging from speech and image recognition, route and transportation resource optimisation and from pattern recognition to robotics and autonomous vehicle technologies. In fact, most of the digital ecosystems that exist today are becoming increasingly smart and intelligent, thanks to the AI revolution. AI technology has also proved that the code is more valuable than the hardware and relies on vast quantities of clean data, appropriate and accurate code and exceedingly high computational resources to produce exceptional results and outputs.

Blockchain as a technology owes its origin to the enigmatic but unknown personality named *Satoshi Nakamoto*. Most people associate blockchain with bitcoin, since the primary purpose of inventing the blockchain was to find a solution to the double spend problem[2] and create a virtual digital currency that requires no third party for verification and attribution. Blockchain can not only be used as an extremely effective way of creating and using digital currency globally, but in fact is a means to create a global ledger, whose contents can be viewed by all, but transactions once entered become immutable and impossible to change. In addition, the blockchain ecosystem is extremely resilient to cyber-attacks and internet blockages. The use of blockchain technology is immense and ranges from land registry platform to tracking movement of diamonds, fissile materials and controlled technology, to the execution of smart contracts.

Big Data is generally characterised by the three Vs i.e. volume, velocity and variety. As more and more data gets generated worldwide, it is becoming increasingly difficult to manage, store, compute and analyse this vast artificial resource. Data, unlike oil cannot be monetised in small quantities. The true value of data emerges only when large quantities of it are processed to generate insights with far reaching consequences, or the unknown unknowns. Storage, management and analytics of Big Data has now become an extremely niche and strategic technology with very few nations in the world possessing the infrastructure, as well as technology, to deal with the ever increasing generation of data in varying formats.

A lot of interest is being generated by quantum computing, as it offers a whole new and fresh approach in dealing with bits (1s and 0s), not as bits which can store either a 1 or a 0 but as a *qbit* or quantum bit that can store both 1 and 0 on the same *qbit*. Thus, the storage and computational power of *qbit* rises exponentially as more and more *qbits* are introduced for storage and simultaneous parallel computation. On October 23, 2019, Google published an article in *Nature* magazine claiming that their quantum computer the *Sycomore* had achieved *quantum supremacy* by solving a unique problem in 200 seconds which the present generation of computers would take 10,000 years to solve.[3] Advances in quantum computing can lead to major breakthroughs like understanding and simulating climate change, or understanding complex protein interactions in the human body leading to development of customised drugs, etc. There are also legitimate concerns that quantum computers would be able to decrypt present generational encryption algorithms, necessitating new ways to provide digital privacy over the internet. US and China are at the fore front of research in this field. However, quantum computing is still very much in its infancy and at the laboratory stage presently because generation of *qbits* and entanglement is an extremely complex process which is carried out at super cooled temperatures. Second, it is very difficult to generate more and more *qbits* and get them entangled. Also, *entangled qbits* can get untangled after sometime, due to noise and other factors. Therefore, we will not be discussing quantum computing and technology any further in this book.

The study and knowledge of cyberspace needs to be imparted to all because this artificial resource is slowly becoming the oxygen for modern living and survival. In addition, for professionals, especially those dealing with policy and government matters, a detailed and nuanced knowledge of the cyberspace domain is a must. However, imparting knowledge of the cyberspace domain is not a trivial matter. First, the subject is extremely vast, complex and fast changing. It is an extraordinary challenge to first grasp the subject in its entirety and thereafter communicate the same in easy language and jargon to a reader who may, or may not, have an engineering background. Second, when companies dealing with this domain provide background information to a policymaker, more often than not, it is limited and brief and biased towards the company's product or the service it provides. This book has been written with the purpose of giving the reader, especially a policymaker, a helicopter overview of the cyberspace domain without bias. In addition, the emerging technologies of AI, blockchain and Big Data are explained with a 360° appraisal of the Indian cyberspace ecosystem.

The book consists of six chapters. In Chapter 2 the reader is introduced to the various definitions of cyberspace, its peculiarities and characteristics along with an overview of the Electromagnetic spectrum, which is one of the most used, but misunderstood natural resource. A detailed account of the cyberspace architecture and building blocks is provided in Appendix A which is crucial for understanding why things are presently the way they are. An overview of global cyberspace challenges including fake news and misinformation campaigns, cybercrime, cyber terrorism and cyber war has also been included in the chapter. Towards the end, the chapter discusses the cyberspace doctrines of USA, China, Russia and India and important cyberspace legislations to include European Union (EU) General Data Protection Regulation (GDPR) and IT (Amendment) Act 2008.

Chapter 3 deals comprehensively with AI. A detailed overview of the AI technology is provided in Appendix B. The chapter covers major sub areas of AI namely, Natural Language Processing (NLP), speech recognition, computer vision/image recognition and robotics. In addition, the latest advancements in AI along with ethical concerns of the technology are also provided. The next two subsections are on use of AI in warfare, its employment as a dual use technology and the important policies of major countries. Towards the end, a brief on the Indian initiatives relating to AI have also been given.

Chapter 4 is divided into two subparts with one subpart dealing with blockchain and the other with Big Data. The subpart on blockchain covers the advent of crypto currencies along with the stand of different countries, including India. Thereafter, an overview of blockchain based smart contracts has been provided. Towards the end, details of India's blockchain ecosystem and initiatives along with use of blockchain in national security has been discussed. The subpart dealing with Big Data is also structured along the same lines as the one dealing with blockchain. After an overview of terminologies and technology, major Big Data analytics platforms like Google cloud, Hadoop and Asterix are discussed. Towards the end, use of Big Data in national security and Indian Big Data initiatives and ecosystem have been discussed.

Chapter 5 offers a detailed appraisal of the Indian Cyberspace ecosystem in ten parts. These are: cyberspace infrastructure; cyberspace governance; government initiatives and digital reforms; defence of cyberspace; cyberspace based economy; cyber-crime; cyberspace related skill sets and workforce; cyber laws; cyberwar; deterrence capacity and capability; and cyber diplomacy.

Finally, Chapter 6 makes certain recommendations pertaining to the Indian cyberspace ecosystem and dares to crystal gaze and give a brief glimpse of the future of the cyberspace domain. The recommended structure of a new Ministry of Cyberspace is given at Appendix C.

Notes

1. For details on the problem, https://www.britannica.com/technology/Y2K-bug, accessed on December 14, 2019.
2. Explained in detail in Chapter 4.
3. For more on the story, https://www.livescience.com/google-hits-quantum-supremacy.html, accessed on December 26, 2019.

2. A Brief Introduction to Cyberspace

Like gods, we have created a new universe called cyberspace that contains great good and ominous evil. We do not know yet if this new dimension will produce more monsters than marvels, but it is too late to go back.

—David Horsey

Introduction

The history of the internet and computers is roughly as old as that of independent India. In December 1947 the transistor was invented, that signalled the development of Integrated Circuit (IC) in 1958-59, which subsequently led to the development of computers and the famous ARPANET network in 1969. It is approximately five decades since the digital network has been in existence and it has completely revolutionised each and every aspect of human life. Alvin Toffler in his 1980 widely acclaimed book *The Third Wave* had described in detail the transition from the 'Hunter Gatherer' to the 'Agrarian' on to 'Industrial' and now the 'Information Age'. It is felt that since early 21st century we have transited from the Information Age to the Instantaneous Age.

Computers and networks have become part and parcel of our everyday life. In fact, most of our day to day gadgets are nothing more but computers in different shapes and sizes. The development of computers and networks has taken place at an extremely rapid pace. In 1965, Gordon E Moore, the co-founder and chairman emeritus of Intel Corporation predicted in a paper that transistor density will double every year.[1] He revised his estimate in 1975 to the number doubling every two years over the next ten years. Revolutionary technological advances in the semi-conductor industry have helped sustain Moore's law, to this date. Along with the advances in Information Technology (IT) hardware, there have also been commensurate advances in the fields of networking technologies and computer applications.

The founders of the internet in 1969 could not have imagined, in their wildest dreams, that their creation would be touching lives of each and every human being in this planet in a short span of just over five decades. The exponential drop in cost of computers, laptops, tablets and smart phones and availability of bandwidth on demand, resulted in more and more people and organisations getting connected to the internet. The resultant explosion of cyberspace placed greater emphasis on connectivity and low costs while overlooking concerns of security and accountability.

Today, cyberspace has become an integral and essential part of human life and organisations. It plays a key role in all critical infrastructure like: power generation and distribution; transportation; strategic industry; finance; telecom and government. It is the major medium of information creation, analysis, storage and retrieval. No corporate organisation can survive without having unhindered access to cyberspace. In a short span of time, cyberspace has become the oxygen on which the global community thrives.

The extraordinary features of cyberspace like instant transfer of information, global reach, standardisation of protocols and applications, anonymity, etc. caught the attention of both state and non-state actors who realised that control and exploitation of this new artificial domain would give them exponential leverage. Defence of cyberspace borders became as important as the protection of land, sea and air borders for nation states. The nations realised that immense harm such as loss of life, property and destruction of critical infrastructure can happen, if an adversary is able to exploit their sovereign and critical cyberspace. The non-state actors, especially fringe groups and terrorist organisations considered cyberspace to be the new war zone where low cost cyber weapons could not only be used for mass destruction, but that the domain was also ideal for conducting psychological operations and other related activities of recruitment, financial transactions and various command and control functions. Cyberspace has been rapidly transformed into a global war zone where innumerable battles are being fought day in and out and adversaries race and compete with each other for fabricating newer and deadlier cyber weapons, coupled with better and stronger protection mechanisms.

Understanding cyberspace is therefore essential for everybody, more so for those dealing with policy and security at all levels. The huge availability of literature coupled with rapid advancements in technology along with a plethora of technical jargon and abbreviations can make this a daunting task. This endeavour seeks to provide an insight into the cyberspace domain and critically examine it in order to crystal gaze into the changing contours of this domain and the way forward for exploiting and defending it.

What is Cyberspace?

Definition

Over a period of time, the term ‘Cyber’ has come to be associated with anything to do with computers, networks, digital, etc. The term is derived from cybernetics which was an engineering field pioneered in the 1940s and concerned the study of communication and control systems in living beings and machines. The term *cybernetics* owes its origin to the Greek word kubernētēs (κυβερνᾶν), meaning ‘steersman’, from *kubernan* ‘to steer’,[2] The term cyber caught the fancy of general public and a large number of variants like cyber punk, cyber rock, cyborg, etc. crept into the English language.

The term cyberspace has no fixed meaning and is interpreted differently by different people, countries, organisations and agencies. The International Telecommunication Union (ITU) does not use the term ‘cyberspace’ but it defines ‘cyber environment’ as including, “users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks."[3] The US National Security Presidential Directive (NSPD-54) Homeland Security Presidential Directive (HSPD-23) defines cyberspace as: "The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries".[4] The CISCO blog by Damir Rajnovic studied the definition of term 'cyberspace' being used by ten different countries/ organisations and made some interesting observations:

- All definitions agree that cyberspace consists of tangible elements.
- All definitions agree that cyberspace must include information.
- Cyberspace includes tangibles, but at the same time is also virtual.
- Contrary to popular belief, networks and internet are desired but not necessarily part or are required for cyberspace.[5]

Ambassador Jayant Prasad, former Director General of Manohar Parrikar Institute for Defence Studies and Analyses (IDSA) defines it as:

> Cyberspace is where information technology and the electromagnetic spectrum come together-its superstructure layered over by the sub-structure of cables, computers, and sea, land and space based communication networks, and energised by the use of information technology.[6]

Daniel T Kuehl defines cyberspace as:

> The global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information – communication technologies.[7]

The definition by Kuehl is by far the most exact definition of cyberspace and comprises of certain important key words as under:

- **Global Domain**: Kuehl defines cyberspace as a domain similar to the other domains of land, water, air and space. However, unlike the natural domains of land, water, air and space, cyberspace is an artificial domain. From a purely military perspective, cyberspace has some interesting attributes. It is a domain which favours the attacker more than the defender. Lack of international laws along with ease of deniability and anonymity assists a weak adversary in inflicting disproportionate harm on a strong and powerful adversary. Creating a cyber weapon is a function of cognitive prowess and intellect, at extremely low material cost. The domain gives a notion of 'virtual space' but, in fact every bit of information generated is stored physically and can be replicated and retrieved. In sum, cyberspace as a domain is a great leveller which favours the underdog and an offensive strategy. Is cyberspace only global? What about the internet connectivity at the International Space Station or the connectivity between the various space crafts and telescopes, orbiting in deep space? It is quite evident that cyberspace is an ever expanding domain which has a reach equal to the reach of human endeavour.
- **Information Environment**: Information is the oxygen of cyberspace ecosystem. Without information, cyberspace is dead. In fact, the quantity and quality of information present in a particular cyberspace ecosystem defines its health or potential.
- **Use of Electronics and Electromagnetic Spectrum**: All activities related to information in cyberspace are carried out with the help of electronics and the electromagnetic spectrum. A library (which also performs information related activities) and consists solely of paper books and periodicals will not form part of cyberspace, as it does not use electronics and the electromagnetic spectrum, to carry out information based activities.
- **Interdependent and Interconnected Networks**: By interdependent and interconnected networks, Kuehl does not only imply networks formed between different computers and devices but also networks formed within a particular computer or device.

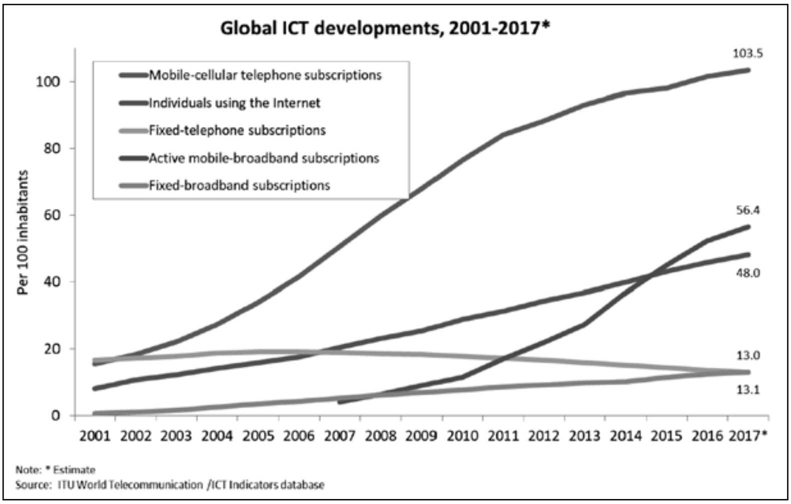
> The various components of a modern computer viz. processor, mother board, memory, ports etc. constitute an interdependent and interconnected network to perform various functions in cyberspace. The value of a network is roughly given by Metcalfe's law which states that the value of a network is directly proportional to the square of the number of interconnected nodes of that network.

For the purpose of this study cyberspace will mean: *An artificial domain consisting of interconnected and interdependent network(s) using electronic and electromagnetic spectrum based Information Communication Technology (ICT) to create, store, modify, exchange and exploit information.*

Peculiarities of Cyberspace

The cyberspace domain has a number of interesting attributes, some of which are discussed below:

- **Artificial Domain**: Being an artificial domain, cyberspace is not constrained by any fixed availability matrix. The domain can be built or dismantled rapidly. Similarly, the potential of the domain to handle information can be increased exponentially by technological advances.
- **Expanding Rapidly**: The last two decades have witnessed a meteoric rise in the internet and information handling capacity of global cyberspace. In 2010, there were a total of 1,991 million internet users in the world. This figure has jumped to 3,385 million in 2016.[8] The global average internet speed was 2.1 MBPS in the first quarter of 2011 which rose to 7.2 MBPS in the first quarter of 2017.[9]
- **Information is Oxygen**: The cyberspace domain is constructed for creating, storing or processing information. The key parameter in judging the efficacy of a given cyberspace domain is its ability to handle information in the fastest, cheapest and most reliable manner. Without information, the cyberspace is just a collection of hardware and software and not a domain. It is estimated that the four big internet companies of Google,



Source: ITU.

Microsoft, Amazon and Facebook currently hold at least 1,200 petabyte of data between them (one petabyte is equal to 10^{15} bytes or 1,000 terabytes).[10]

- **Instant Global Access**: The internet is expanding rapidly and is being used by more than half of the global population. In 2000, only 9.45 per cent of the global population was using the internet, while in 2016, 52.05 per cent of the global population has access to internet.[11]
- **Dependence on Intellectual Property and Technology:** Cyberspace is heavily dependent on contribution from academia, industry, governmental and non-governmental organisations. A large number of applications and technologies of cyberspace have been patented with different organisations vying with each other to shape the present and future contours of cyberspace. Intellectual property and technology play a major role in the exploitation and expansion of cyberspace. This is necessary as it fuels innovations and rewards early achievers but, on the flip side it has led to patent wars and rival buy outs by major firms to maintain their monopoly. In recent years firms are applying for large numbers of patents and using them in innovative ways

as part of their overall corporate strategy. Patents are used to generate revenue through licencing, signalling innovativeness to shareholders and blocking the patent applications of rival firms.

- **Commonality of Basic Building Blocks**: The entire cyberspace ecosystem is fully standardised. Most of the ICT standards are set by the ITU and Institute of Electrical and Electronics Engineers (IEEE), 3 Park Avenue, New York.
- **Impacts Everyone and Everything:** Presently, more than half the global population is connected to cyberspace. There is hardly any region on the planet including outer space, that is not utilising cyberspace to perform one or more functions. Because of exponentially decreasing cost of smart phones and data rates, more and more people are accessing the internet and utilising it for innumerable purposes. The meta data being generated continuously is being utilised for extracting intelligence for further fuelling innovation and invention, in diverse fields of health care, governance, education, science, etc.
- **Low Cost of Entry**: The exponential increase in information storage capacity and faster processing speeds coupled with the large volumes and better manufacturing processes, has ensured that the costs of essential ICT devices for accessing cyberspace have decreased rapidly. Hard drive prices have dropped from $500,000 per gigabyte in 1981 to less than $0.03 per gigabyte in 2018.[12] In 2001, it used to cost $10,000 per one megabyte of raw DNA data which is almost free today.[13]
- **Lack of International Laws**: Cyberspace is a global domain which is presently weakly regulated and lacks common international laws. In 1998, the Russian Federation introduced a draft resolution on 'Developments in the field of information and telecommunications in the context of international security' which was adopted without a vote by General Assembly as Resolution 53/70. Since then, there have been annual resolutions seeking the views of member states on information security. In addition, four Groups of Governmental Experts (GGE) have been convened since 2004 to examine the existing and potential threats from cyberspace and the possible international cooperation measures. The first 15-member GGE could not

agree on a substantive report. The second 15-member GGE was established in 2009 and a report was issued in 2010 (A/65/201). The second GGE recommended the following: (a) Dialogue on norms for state use of ICT to reduce risk and protect critical infrastructure; (b) Confidence building and risk reduction measures; (c) Information exchange on national legislations and national ICT security strategy, policies and technologies; (d) Capacity building in less developed countries; and (e) Elaboration of common terms and definitions on information security. The third GGE functioned during 2012/13 and submitted its report to the UN General Assembly in June 2013. It agreed on the following: (a) International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful and accessible ICT environment; (b) State sovereignty applies to the state's conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory; (c) State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms; (d) States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-state actors for unlawful use of ICTs; and (e) The UN should play an important role in promoting dialogue among member states.[14] The fourth GGE functioned from July 2014 to June 2015 and its report was published on July 22, 2015. The GGE proposed three potential "voluntary non-binding norms" for state behaviour in cyberspace: (a) States should not attack each other's critical infrastructure for the purpose of damaging it; (b) States should not target each other's cyber emergency response systems; and (c) States should assist in the investigation of cyber-attacks and cyber-crimes launched from their territories when requested to do so by other states.[15] In addition, two more GGE were established, one in 2016/17 (vide UN Resolution A/RES/70/237) and another in 2019/21 (vide UN resolution A/RES/73/266).

In December 2018, the UN General Assembly vide resolution A/RES/73/27 established an Open Ended Working Group (OEWG) with the charter to focus their discussions along six broad agendas. These are: existing and potential threats; international laws; rules, norms and principles; regular institutional dialogues; confidence building measures; and capacity building. The OEGW is expected to submit its report to the 75th session of the UN GA being held from September 15-30, 2020.[16]

Towards end 2009, an international group of legal and cyber experts led by Professor Michael N Schmitt, Chairman United States Naval War College were invited by the Tallinn based NATO Cooperative Cyber Defence Centre of Excellence, to study how international law (in particular the *jus ad bellum* and International Humanitarian law) applied to cyber conflicts and cyber warfare. The outcome was the *Tallinn Manual 1.0* which was published on March 15, 2013. The manual is divided into sections referred to as "black letter rules" and the accompanying commentary. Subsequently, the *Tallinn Manual 2.0* which further expanded on the scope of the *Tallinn Manual 1.0* was published by Cambridge University Press in February 2017.[17] *The Tallinn Manual 2.0* consists of 154 rules and lays down the legal framework for conduct of cyber operations by states in land, sea, air and space, in detail. The manual is not endorsed by either the NATO, the UN or any other state/alliance.

- **Anonymity and non attributability**: The basic reason for the anonymity on the internet is related to the way the internet is created and governed. The primary purpose of internet creation was to enable digital interconnectivity between disparate devices in a seamless and simplistic manner. The focus was to ensure the reliability of connectivity and interoperability of multiple devices. There is always a trade-off between simplicity and security. Security comes at extra cost and requires additional complexities to be built in with stringent requirements relating to data rates, processor speeds, memory and network efficiencies. Without security, the system is cheaper, requires less memory and processing speeds, works faster and can sustain more degradation in communication channels. Hence, simplicity over security was preferred by the ICT industry for a long time, till cyber-crime and national security concerns took centre stage and just could not be ignored or dismissed.

The challenge of doing away with anonymity on the internet is less of a technical and more of a cultural, political and diplomatic issue. There are presently no rules barring a person/group/organisation/machine from creating multiple personalities/accounts/profiles on multiple devices without real life governmental authentication. It can be considered analogous to driving multiple cars simultaneously across the world, with no licence plates. People sometime wrongly confuse anonymity with privacy. A real identified person can encrypt his mail to retain privacy. Right to privacy is contingent on non-anonymity. Adam Firestone has beautifully summed it up by saying, "Transparency and accountability promote civil, courteous behaviour. Anonymity tempts people to behave poorly, creating a culture of 'if I can't be identified, I can't be caught'".[18] Personalised cyberspace which has been created by individuals/organisations/groups for their own needs is generally very tightly regulated with almost zero chance of anonymity. Anonymity to some extent is also encouraged by multinational IT companies, as their revenue models generally revolve around number of virtual user/accounts, and not on the number of actual user/accounts.

Attributing a cyber incident to a particular individual or group is exceedingly difficult. First, cyber-attacks can be carried out from multiple geographical independent locations by multiple persons and machines. Second, in a number of cases, particularly in Distributed Denial of Service (DDoS) types of attacks, the machines carrying out the attack are remotely exploited without permission or knowledge of the IT resource owner. Thirdly, cyber-attack tools can be clandestinely obtained from a number of sources and thereafter the same tools can be utilised to carry out damaging cyber-attacks. The US has made attributability of cyber-attacks a focus point of their cyber strategy. The 2015 US Department of Defence (DOD) Cyber Strategy document states:

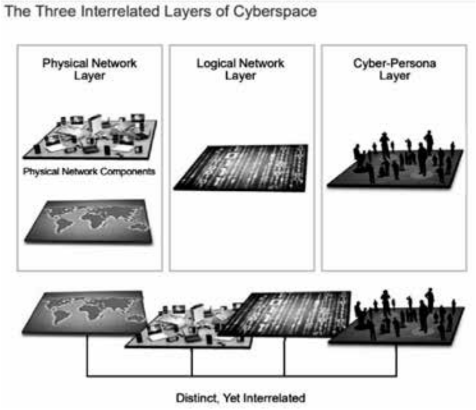
> Attribution is a fundamental part of an effective cyber deterrence strategy as anonymity enables malicious cyber activity by state and non-state groups. On matters of intelligence, attribution, and warning, DoD and the intelligence community have invested significantly in all source collection, analysis, and dissemination capabilities, all of which reduce the anonymity of state and non-state actor activity in cyberspace. Intelligence and attribution capabilities help to unmask an actor's cyber persona, identify the attack's point of origin, and determine tactics, techniques, and procedures.[19]

On December 19, 2017, the White House in its press briefing meeting attributed the origin of *Wannacry* ransomware to North Korea.[20] The *Wannacry* ransomware did not propagate through the usual route of clicking an unknown e-mail attachment. It exploited two cyber-attack tools *EternalBlue* and *DoublePulsar* to address Server Message Block (SMB) port 455 vulnerability in the *Windows* family of operating systems to gain entry into computers which had not been patched and subsequently propagated to other computers and networks. Both the cyber-attack tools *Eternal Blue* and *Double Pulsar* were developed by US National Security Agency (NSA) and leaked online by the 'Shadow Broker' hacker group on April 14, 2017.[21] As can be seen from the above, the tools developed by the security agency of one country were used by a second country, to launch worldwide cyber-attacks. Whom do you then finally attribute the attack to?

- **Exponential First off the Block Advantage**: The ICT industry has always exponentially rewarded the first off the block, innovator. This is amply evident in the way mega ICT corporations garner the major portion of the business pie, wage open patent wars and undertake mergers and acquisitions in order to ensure that no worthwhile competition survives in their major vertical of the cyber domain. The ICT industry can be broadly classified into two primary verticals: the hardware and software. The hardware vertical consists of microprocessors and integrated circuit chips, routers, servers, firewalls and other networking components. The software vertical, includes operating systems, browsers, e-commerce platforms and various application systems concerning social networks, office procedures and high end industry specific applications. Intel Corp. founded in 1968, was the first company to develop and produce semi-conductor based integrated circuits and chips. It introduced the Pentium processor in 1993 that revolutionised the Personal Computer (PC) industry. Till date, it is the world leader in PC processors and has a market share of 79.4 per cent.[22] Facebook was the first social networking site in the world. It is also the most used social networking site today with monthly active users numbering 2,23,00,00,000.[23]

- **Multiple Stakeholders**: The US Joint Publication 3-12 *Cyberspace Operations* describes cyberspace as being composed of three layers, i.e. the physical, logical and cyber-persona.[24] The physical layer comprises of all the hardware elements like, switches, cables, computers, mobiles, routers, etc., while the logical layer comprises of the software portion or various operating systems and applications that are used to store, modify, analyse, move and destroy information. The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another.

More than 90 per cent of the cyberspace is owned by private entities and players from around the world. There is no country which can claim that its entire cyberspace is indigenous. This attribute of the cyberspace affords faster innovation and free flow of concepts and ideas. However, it gives certain companies and governments, who have a major say in design, development, standardisation, production and marketing of the components of physical and logical layers of cyberspace an immense advantage over other players, which can be exploited immensely.


The Three Interrelated Layers of Cyberspace
Physical Network Layer
Logical Network Layer
Cyber-Persona Layer
Physical Network Components
Distinct, Yet Interrelated

Source: US DOD Publication JP 3-12

- **Difficult to defend and easy to attack:** The internet was conceived and developed as primarily a network capable of transferring information from one computer to another. Security was not in built into the basic building blocks. It is only later when the technology stabilised and expanded rapidly, did people started worrying about the security aspects of the ICT networks. The first virus was created as a joke by high school student Rich Skrenta, in early 1980s, and affected the DOS 3.3 operating system.[25] Since the current cyberspace is an off shoot of the earlier models of internet, it continues to be largely built on the seven layer of the Open Source Interconnection (OSI) model, developed by the International Standards Organisation (ISO) in 1984. The cyberspace is vulnerable at all its three layers of physical, logical and cyber-persona and a breach in one layer can have a cascading effect on the other layers as well. Since the cyberspace architecture is standardised with limited niche players controlling bulk of the cyberspace domain, a single undetected vulnerability can compromise a large number of genuine cyberspace users. It is therefore evident that the cyberspace heavily favours the attacker than the defender, with multiple vulnerabilities surfacing each and every moment. As a corollary to the above, the cost of procuring a highly sophisticated cyber-attack weapon is very little, compared to the cost of defending an important and critical cyberspace network.

A comparative study between the attributes of various domains with the cyber domain is given below:

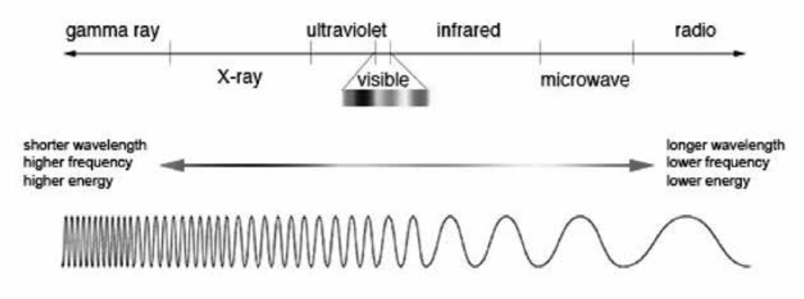
Attribute	Land	Water	Air	Space	Cyber
Natural/ Artificial	Natural	Natural	Natural	Natural	Artificial
Key Ingredients	Soil, Minerals, Flora	Water	Air	Vacuum	Hardware, software, digital networks
Inter State Borders	Well Defined	Well Defined	Well Defined	Not Defined	Not Defined
Means of transportation	Foot, animals, cars, buses, train etc	Boats, ship, submarine	Aircraft, balloon	Spacecraft, rocket	Mobile, computer, smart device etc
Max Speed of transportation	1,228 km/h	511 km/h	8,000 km/h	58,000 km/h	2,200 km/ sec
Number of transportation vehicles	Many	Less than Land	Less	Extremely less	Too many

Electromagnetic Spectrum: An Important Constituent of Cyberspace: The cyberspace uses electronics and the electromagnetic spectrum for performing varied tasks relating to information. Thus, an overview on the electromagnetic spectrum and its correlation with data rates and bandwidth is essential for understanding the broad contours of cyberspace.

- **Electromagnetic (EM) Waves**: These are synchronised oscillations of electric and magnetic fields which propagate at the speed of light. The entire cosmos is filled up with EM waves and these constitute an equally distributed natural resource with multiple applications and uses. The electric and magnetic fields are perpendicular to each other and the direction of propagation of the wave is perpendicular to both the fields.

  Frequency (f) of a wave is defined as the rate of oscillation of a wave and is measured in hertz (Hz). One Hz is equal to one oscillation per second. Wavelength (λ) is the distance between two adjacent crests or troughs of a wave. The frequency is inversely proportional to the wavelength and is expressed as c = f λ. Where c is the speed of light. EM radiation is classified by wavelength into radio, microwave, infrared, visible, ultraviolet, X ray and gamma rays.

Attenuation (loss of energy) is directly proportional to frequency. It implies that lower band of frequencies travel farther as compared to higher band of frequencies. In addition, the extremely higher end of the EM spectrum have higher energies which are harmful for living beings. Thus, the radio, microwave, infrared and visible range of the spectrum are used for communication purposes.



Source: NASA's Imagine the Universe

- **Relationship between frequency, bandwidth and Data Rate**: Bandwidth is the range between the highest and lowest frequencies being carried by a communication channel. Typically, it is 10 per cent of the centre frequency of the channel. So, a radio frequency operating at centre frequency of 60 Mega Hertz (Mhz), has roughly a bandwidth of 6 MHz.

  Conversion of digital information (1s and 0s) for transmission over the EM spectrum involves manipulating either the frequency, amplitude or phase of the spectrum. Thus, one can transmit a particular frequency to denote a '1' and another frequency to denote a '0'. In 1927, Nyquist[26] determined that the number of independent pulses that can be put through a telegraph channel (communication channel) per

> unit time is limited to twice the bandwidth of that channel or fp ≤ 2B, where fp is the pulse frequency and B is the channel bandwidth. This implied that the bandwidth places a major restriction on the number of bits which can be error free transmitted over a communication channel. Let us take a simplified example of a transmitter – receiver system operating with a centre frequency of 60 Mhz. Thus, its bandwidth is roughly 6 Mhz or 60,00,000 hertz and the maximum bit rate it can support is 12 MBPS. This is the reason why microwave, satellites and OFC are used as backbone carriers for backhaul communications because of their high operating frequencies, which results in larger bandwidth and thus larger information carrying capacity.

A detailed tutorial on cyberspace architecture and building blocks that includes network topologies, basic hardware and software building blocks, addressing schemes, mobile communications, security and cryptology is given at Appendix A.

Internet Governance

Introduction: The Working Group on Internet Governance (WGIG) defined Internet Governance as: "Internet Governance is the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the internet."[27] The internet is a major subset of cyberspace and it goes without saying that in today's world, the state/ institution which has a majority stake in controlling this artificial resource will yield enormous power and influence globally.

The WGIG was set up by the UN Secretary-General based on the mandate accorded to him during the first phase of the World Summit on the Information Society (WSIS) held in Geneva from December 10 to 12, 2003. The WGIG comprised of 40 members from government, private sector and civil society and was chaired by Mr Nitin Desai, special adviser to the Secretary-General for the WSIS.

The working group identified four key policy areas which were extremely relevant for internet governance. These were:

- Issues relating to infrastructure and management of critical internet resource to include administration of Domain Name Service (DNS), allocation of IP addresses, administration of root server systems, technical standards, peering, interconnections and telecommunication infrastructure.
- Issues relating to the safe use of the internet like combating spam, cyber-crime and network security.
- Issues that are common to the internet and other business areas like Intellectual Property Rights (IPR) and international trade and for which there are existing organisations.
- Issues relating to the developmental aspects of internet governance especially capacity building in developed countries.

Some of the major problem areas presented before the WGIG were:

- Unilateral control of the US government on root zone files and systems.
- Varied and uneven distribution of interconnecting costs, which were higher for developing countries vis-à-vis the developed ones.
- Lack of organisations and mechanisms to ensure network stability, security of infrastructure and preventing cybercrime.
- No unified approach towards combating spam.
- Lack of transparency, openness and global participation in policy development.
- Inadequate capacity building efforts especially in developing countries.
- Lack of policy and procedures towards allocation of top generic Domain Names and IP addressing schemes.
- Varied problems of IPR, freedom of expression, data protection, multilingualism, privacy and consumer rights.

The WGIG defined the roles and responsibilities of governments, the private sector and civil society as under:

- **Governments:** The major roles and responsibilities included the following:
  - Public policy making, coordination and implementation at the national, regional and international level.

  - Creating an enabling environment for ICT development.
  - Performing oversight functions.
  - Formulation of laws, regulations and standards.
  - Promoting access to ICT services, capacity building and best practices.
  - Combating cybercrime.
  - Dispute resolution and arbitration.
- **The Private Sector:** Some of the major roles and responsibilities were as under:
  - Self-regulation by the ICT industry.
  - Development of best practices.
  - Formulation of policy proposals, guidelines and tools for policymakers and other stake holders.
  - Research and Development (R&D) of technology, standards and processes.
  - Fostering innovation.
  - Contributing towards drafting of national laws and participation in national and international policy making.
- **Civil Society:** Some of the major roles and responsibilities of the civil society are:
  - Capacity building through knowledge, training and skill sharing.
  - Promoting various public interest initiatives.
  - Giving the government and the private sector perspective of marginalised groups.
  - Engagement with the government and private sector in policy and law formulation.
  - Contributing expertise, skill, experience and knowledge in a range of ICT policy areas.
  - Development and dissemination of best practices in the field of ICT.
  - Attempting to ensure that political and market forces are accountable to the needs of all the members of civil society.
  - Ensuring social responsibility and good governance practice.

The WGIG in their report remarked that any organisational structure dealing with internet governance should adhere to the following three principles:

- No single government should have a pre-eminent role in international internet governance.
- The organisation for internet governance will be multilateral, transparent and democratic with full involvement of governments, the private sector, civil society and international organisations.
- The organisation for internet governance will involve all stakeholders and relevant inter-governmental and international organisations.

The WGIG report proposed four models of internet governance along with a host of other recommendations which were taken note of by various stakeholders but due to lack of consensus, did not materialise into structures on ground.

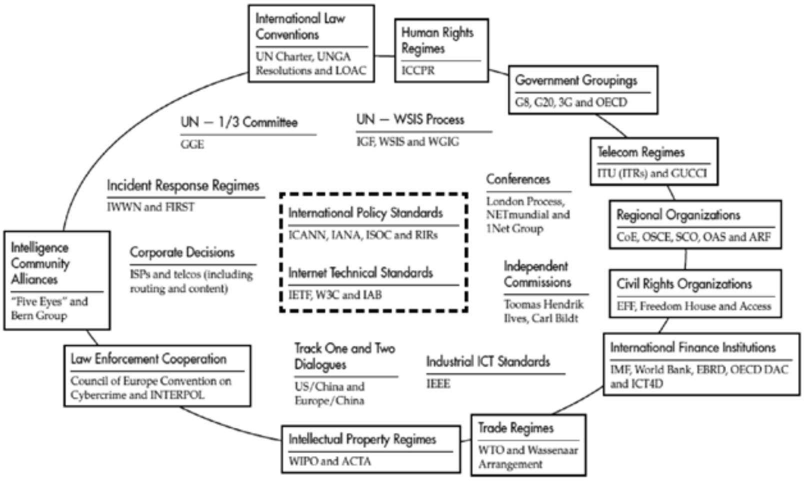
Current System of Internet Governance: Before moving to the various organisations and institutions responsible for carrying out global internet governance, there is a need to understand the concept of *norms* and *regimes* from the cyberspace perspective. The definition of a norm is "a collective expectation for the proper behaviour of actors with a given identity."[28] Norms are thus, shared beliefs within a community. Having commonly acceptable norms in the cyberspace domain are difficult as the number of stakeholders are many and agreeing on collective set of norms becomes a major challenge. It is also pertinent to mention that the standing/reputation/value of the group promulgating norms is a major leverage for ensuring that all major stakeholders agree on the common agreed norms as exclusion from the group may result in major tangible setbacks for the members. It would therefore imply that norms agreed to by the UN will carry more weightage compared to the norms agreed to by less influential groups. The bilateral agreement of 2015 between US and China against cyber espionage for commercial advantage resulted in similar agreement between the G20 nations and is an acceptable norm amongst a large number of nations.

Principles on the other hand are like vision statements which provide a bigger picture and afford greater leeway to members in comparison to norms, which are more specific and detailed. Laws on the other hand are more precise than norms. Due to the large number of stakeholders in the cyber domain, the present emphasis is on voluntary norm creation and acceptance.[29]

Regimes can be described as the set of rules, norms, principles and procedures that define the building blocks of a complex ecosystem like cyberspace. According to Nyle,[30] a regime complex is a loosely coupled set of regimes.

The figure below depicts the regime complex for managing global cyberspace. The figure does not denote all the organisations and institutions responsible for managing global cyber activity, but is an indicator of the sheer scale and complexity involved in running the global cyberspace ecosystem. Some of the important organisations dealing with internet governance are discussed in subsequent paragraphs.

The Regime Complex for Managing Global Cyber Activity


International Law Conventions
UN Charter, UNGA Resolutions and LOAC
Human Rights Regimes
ICCPR
Government Groupings
G8, G20, 3G and OECD
UN – 1/3 Committee
GGE
UN – WSIS Process
IGF, WSIS and WGIG
Telecom Regimes
ITU (ITRs) and GUCCI
Incident Response Regimes
IWWN and FIRST
Conferences
London Process, NETmundial and 1Net Group
International Policy Standards
ICANN, IANA, ISOC and RIRs
Regional Organizations
CoE, OSCE, SCO, OAS and ARF
Intelligence Community Alliances
"Five Eyes" and Bern Group
Corporate Decisions
ISPs and telcos (including routing and content)
Internet Technical Standards
IETF, W3C and IAB
Independent Commissions
Toomas Hendrik Ilves, Carl Bildt
Civil Rights Organizations
EFF, Freedom House and Access
International Finance Institutions
IMF, World Bank, EBRD, OECD DAC and ICT4D
Law Enforcement Cooperation
Council of Europe Convention on Cybercrime and INTERPOL
Track One and Two Dialogues
US/China and Europe/China
Industrial ICT Standards
IEEE
Trade Regimes
WTO and Wassenaar Arrangement
Intellectual Property Regimes
WIPO and ACTA

Source: Joseph S. Nye, Jr[31]

International Telecommunication Union:[32] The ITU was founded in Paris in 1865 as the International Telegraph Union and in 1947 became a specialised agency of the United Nations dealing with ICT.

ITU has three main areas of work (also known as sectors) namely radio communications (to include allocation of radio spectrum, satellite orbits, etc.), standardisation (for developing global ICT standards for internet access, protocols, voice and video compressions etc.) and development (formulation of internet policy frameworks, publishing ICT statistics and undertaking various initiative aimed at bridging the digital divide).

The mission of ITU Radio Communication Sector (ITU-R) is to ensure the rational, equitable, efficient and economical use of the Radio Frequency (RF) spectrum by all the radio communication services including those using satellite orbits. The ITU-R allocates bands in the RF spectrum and radio frequencies associated with orbital positions in the geo-stationary orbit, in order to avoid harmful interference between different users of the RF spectrum.

The ITU-R provides the Maritime mobile Access and Retrieval System (MARS) database which gives out the station name, call sign and frequencies assigned to ship stations and coast stations; and Maritime Mobile Service Identity (MMSI) assigned to Aids to Navigation (AtoN) platforms and Search and Rescue (SAR) aircrafts. In addition, it also provides the Global Administration Data System (GLADS) and BR International Frequency Information Circular (BR IFIC) of space services as well as terrestrial services, which are published every two weeks and give out information on the frequency assignment to space stations, earth stations, radio astronomy stations and all terrestrial stations which are then submitted to the Radio Communication Bureau for recording in the Master International Frequency Register. It also provides information on various patents pertaining to the radio communication sector, the Space Network List (SNL) which gives basic information concerning planned or existing space stations, earth stations and radio astronomy stations and maintains the Space Network Systems (SNS) database.

The ITU-R is sub-divided into the Space Services Department and the Terrestrial Department. It is also currently hosting seven study groups on spectrum management, radio wave propagation, satellite services, terrestrial services, broadcasting services and science services.

The ITU's Telecommunication Standardisation Sector (ITU-T) forms a number of study groups which invite experts from all corners of the globe to develop international standards, known as ITU Recommendations. These standards then define the basic structures of the global information and communication ecosystem. Presently, a large number of study groups on operational aspects, economic and policy issues, environment and circular economy, broadband cable & TV, protocols and test specifications, future networks, multimedia, security, IoT, smart cities and communities are functioning in ITU-T.

The Telecommunications Development Sector (ITU-D) focuses on the creation, development and improvement of ICT equipment and networks, particularly in developing countries. The ITU-D's secretariat known as the Telecommunication Development Bureau (BDT) which is sub divided into four departments. These are: the Administration and Operations Coordination department; the Infrastructure, Enabling Environment and e-applications department; the Innovation and Partnership department; and finally, the Projects and Knowledge Management department.

Internet Engineering Task Force (IETF):[33] The IETF is an open international community of network designers, operators, vendors and researchers who are interested in the evolution of the internet architecture and its smooth and efficient operation. The task force is open to any individual who wishes to join it.

The IETF works through the medium of working groups with each group focusing on a particular area or topic (routing, transport, security, etc.). Each working group is headed by an Area Director or AD who is a member of the Internet Engineering Steering Group (IESG). In addition, there is an Internet Architecture Board (IAB) which provides architectural oversight, an Internet Research Task Force (IRTF) and an Internet Society (ISOC). Most of the IETF's working is through internet and only three meetings are held in a year.

The Application and Real Time Area (art) is responsible for developing the application protocols and architecture and falls under three categories. One focuses on development of protocols and architecture to support delay sensitive interpersonal communications like voice, video, instant messaging etc.; the second on protocols and architecture to support applications which are not delay sensitive like HTTP, email, FTP, etc.; and the third category consists of common building blocks which can be used by both delay sensitive and delay insensitive applications like authentication mechanisms, data formats, metrics and codecs. The General Area (gen) is responsible for overseeing the IETF standards development process. The Internet Area (int) covers topics relating to IP layers (Ipv4 and IPv6), DNS, DHCP, host and router configuration, mobility, MPLS and other Link Layer technologies. The Operations and Management Area (ops) covers topics relating to network management like DNS operations, IPv6 operations, operational security and routing operations. It also takes regular feedback from Internet Service Providers (ISP) about the performance of various network management functions. The Routing Area (rtg) is responsible for ensuring efficient operations of the internet routing system and developing new protocols and extensions including bug fixing. The Security Area (sec) focuses on the various security protocols and services of integrity, authentication, non repudiation, confidentiality and access control. The Transport Area (tsv) deals with a range of topics dealing with data transport over the internet including various congestion control algorithms.

The Internet Cooperation for Assigned Names and Numbers (ICANN):[34] The ICANN is a non profit organisation responsible for efficient management and administration of a number of databases pertaining to the management of protocol parameters, internet numbers, resources and domain names.

The internet depends on a unique identifier which is the IP address of a database/application/web page/portal on the world wide web. Rather than writing the actual IP addresses on the web browsers, they are translated into the domain names which are easily remembered and understood. When a person using the web browser clicks on a domain name, the information first goes to a server which translates the name into the IP address which further directs the user to the web site's network location. The ICANN is responsible for allocating internet number resources, creating registries which map IP addresses to domain names, run the Domain Name Servers and publish all registries in the open domain for general public use. It is also responsible for introduction of new generic Top Level Domains (TLD) which is the highest level in hierarchical Domain Naming System. The TLD names are installed in the root zone of the name space. Some of the examples of Top Level Domains are .com, .edu, .org, .in IANA currently classifies TLDs as country code TLD, generic TLD (which can be sponsored or un-sponsored) and infrastructure TLD (.arpa).

The generic TLDs have three or more characters. The sponsored TLDs are proposed and sponsored by private agencies or organisations who formulate and enforce their own rules concerning use of that TLD. The country-code TLDs are two lettered domain names for countries or territories. Barring a few exceptions, the code for countries is the same as its ISO 3166 code.

The ICANN was established as a corporation on September 30, 1998 and incorporated in the US state of California. Before establishment of ICANN, its functions were being performed by Jon Postel who was a computer science researcher and was part of the team that created ARPANET. ICANN was based on a green paper published by US National Telecommunication and Information Administration (NTIA) agency under US Department of Commerce. Till October 1, 2016, ICANN managed the Internet Assigned Numbers Authority (IANA) under contract to the US Department of Commerce and with an agreement with IETF.

On October 7, 2013, the Montevideo Statement[35] was issued by heads of top organisations (known as I* group) dealing with governance of the internet's global architecture. It was the fallout from the Snowden revelations which detailed the mass surveillance of internet traffic by NSA and intelligence agencies of other partner countries. The statement:

> … expressed strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance" and "called for accelerating the globalization of ICANN and IANA functions, towards an environment in which all stakeholders, including all governments, participate on an equal footing.

The signatory organisations included ICANN, IETF, IAB, World Wide Web Consortium, the Internet Society and five regional internet address registries.

World Wide Web Consortium (W3C):[36] The W3C was founded by Tim Berners-Lee, inventor of World Wide Web in October 1994. The organisation was raised at Massachusetts Institute of Technology laboratory of Computer Science with support from the European Commission and DARPA. The consortium is jointly run by MIT Computer Science and Artificial Intelligence laboratory (CSAIL), the European Research Consortium for Informatics and Mathematics (ERCIM), Keio University (Japan) and Beihang University (China). The main purpose of W3C is to formulate common standards for the web technologies. The broad process followed before arriving at a standard is as under:

- Common interest in a particular topic is arrived at by taking feedback from the general public, members of W3C and other institutes, industry and organisations.
- W3C then formulates an Activity Proposal which lays down the scope, duration and other characteristics of the project work. After multiple deliberations, the Activity Proposal is sanctioned by the Director.
- Thereafter Working Groups with member representatives, invited experts and team representatives are constituted to commence work on the Activity proposal.
- After multiple iterations and review by members and public, the Advisory Group reviews the technical report submitted by the working group and publishes it as a recommendation.

International Watch and Warning Network (IWWN): IWWN was established in 2004 as a collaborative exercise by 15 countries to combat cyber threats and address vulnerabilities. The member countries of IWWN are: Australia, Canada, Finland, France, Germany, Hungary, Italy, Japan, The Netherlands, New Zealand, Norway, Sweden, Switzerland, United Kingdom and United States of America. The US Department of Homeland Security along with IWWN conducted an international exercise *CYBERSTORM IV* from March 20 to 21, 2013 to practice and test procedures for an international response to a global cyber attack.

Forum of Incident Response and Security Teams (FIRST):[37] FIRST was established in 1990, post the global cyber-attack of *Wank Worm* in October 1989 which highlighted the criticality of timely coordination and action between the cyber response teams of different countries to successfully mitigate a cyber-attack. It is an international organisation consisting of 449 teams in 90 countries formed with the purpose to effectively combat cyber threats, share technical information, tools, methodologies, processes and best practices in order to promote a safer and more secure global electronic environment. FIRST hosts multiple Special Interest Groups, where member teams participate and collaborate to share expertise and experience in the specified area of interest. Each group regularly publishes a host of important open source material dealing with best practices, cyber incident analysis and detection techniques, incident response training and exercises and cyber security tools. In addition, FIRST participates actively in United Nations sponsored Internet Governance Forum as a technical expert.

International Criminal Police Organisation (INTERPOL): INTERPOL is a global inter-governmental organisation of 194 member countries formed with the purpose of information sharing and combatting international crime. All the member countries are connected on an exclusive communication network called I-24/7. The organisation is divided into three major verticals – counter terrorism, organised and emerging crimes and cyber-crimes. The agency is headquartered at Lyon, France and has a Global Complex for Innovation (GCI) at Singapore. As far as cyber-crimes are concerned, INTERPOL provides three tiered support. Firstly, it helps countries to conduct investigations for which it also has state of art digital forensic capabilities. Secondly, it launches counter cyber-crime operations and has a Cyber Fusion centre operational round the clock for actionable intelligence. Lastly, INTERPOL provides training on combatting cyber-crimes to member countries.

Institute of Electrical and Electronics Engineers:[38] IEEE was established on January 1, 1963 after the merger of American Institute of Electrical Engineers and Institute of Radio Engineers and is the world's largest association of technical professionals with more than 4,17,000 members in over 160 countries.

IEEE has 39 technical societies and seven technical councils and publishes approximately 200 transactions, journals and magazines annually, which is one third of the world's technical literature in electrical engineering, computer science and electronics. It is also a leading developer of international standards of telecommunication, IT and power generation products and services. The IEEE standards association has a portfolio of more than 1,300 standards with over 660 under development standards. It includes the famous IEEE 802 standard of Wi-Fi.

Table of some of the important internet governance organisations along with their charter is given below:

Internet Governance Organisations

Organisation	**Subject Matter Jurisdiction**
Internet Corporation for Assigned Names and Numbers (ICANN), which includes function referred to as the Internet Assigned Numbers Authority (IANA)	Supervises the Domain Name System, allocates internet protocol address space and oversees the root zone servers that provide basic finding information for internet traffic
Internet Society and related organisations : Internet Engineering Task Force (IETF), Internet Engineering Steering Group (IESG) and Internet Architecture Board (IAB)	Develops standards for operation of Internet and its overall architecture
World Wide Web Consortium	Develops standards for the World Wide Web
International Telecommunication Union (ITU)	Develops standards for telecommunications, including interface of internet and telecommunication systems
Organization for Economic Cooperation and Development, European Union, Council of Europe, United Nations agencies	ad hoc policy development on issues of critical interest to members

National governments acting individually or through joint agreements	Ad hoc policy development chiefly related to cyber crime, use and commercial regulatory issues
Institute of Electrical and Electronics Engineers, International Electrotechnical Commission, International Organization for Standardization	Standards for products and for manufacturing and testing processes (operations of these entities relate only peripherally to the operation of the Internet itself)

Source: Harold Kwalwasser, *Internet Governance*, edited by Franklin D. Kramer, Stuart H. Starr and Larry Wentz, *Cyber Power and National Security*, New Delhi: Vij Books, June 2009.

Global Cyberspace Challenges

Cyber-Crime Terminologies: The advent of internet also saw the rapid rise of cyber-crime and cyber-attacks across the globe. Since the early days of internet were focussed on connecting the network rapidly across multiple platforms with least cost in terms of equipment, software, memory, processing speed and data rates, very little attention was given to cyberspace security. This enabled early hackers to get relatively easy access to systems and exploit them for causing disruptions, defacement and losses. As the internet proliferated rapidly and gave rise to new verticals of e-commerce, e-finance and social media, there was a considerable jump in cyber-crimes which led to the governments, banks, multinational companies and developers getting their act together and developing multi layered security systems and architecture. The revelations of Edward Snowden in 2013, brought into world focus the enormity of mass surveillance being carried out by a number of governments and raised important questions on digital privacy and freedom.

Some of the important terminologies being used in the field of cyber-crime[39] are as under:

- **Botnet:** Short form of *Robot Network*. A network of compromised computers which have been infected by malicious software and are discreetly working under the control of a cyber-criminal.

- **Catfish:** False images of personalities created in order to entice and lure users on social media sites.
- **Clickjacking:** Act of tempting internet users to click links containing malicious software or unknowingly share private information on social media sites.
- **Dark Web:** The illicit or hidden portion of the internet which requires special programmes and browsers for access. The Dark Web affords anonymity and confidentiality to the surfer and is used widely for illegal activities ranging from drugs, prostitution, sale of confidential data and trade secrets and transfer of money.
- **Denial of Service (DOS) Attack:** The deliberate act of overloading a particular service like website, traffic route etc. from multiple computers and routes with the aim of disrupting that service.
- **Honeypot:** A security feature built into the network to lure hackers into meaningless locations in order to prevent attack on critical systems and data.
- **Malware:** Short form of *Malicious Software*. A computer programme designed with an intent to carry out illegal activity like eavesdropping, gaining unauthorised access, deceiving network users, destroying/disrupting computer resources, etc.
- **Man in Middle Attack:** In this kind of attack, the messages between two parties are intercepted during transit and thereafter relayed after a miniscule gap so that the parties get the impression that they are passing information end to end, while in reality the information is first being intercepted and then forwarded. The information being intercepted in the middle could be used for intelligence gathering or content alteration.
- **Phishing:** Act of duping users into divulging their sensitive information by creating fake websites of genuine web portals like e-commerce, banking sites, etc.
- **Ransomware:** A form of malware which first hijacks a computer's data (by encrypting it) and thereafter posts a message demanding money (usually in form of bitcoins) to restore it.
- **Spoofing:** The act of fooling a user into believing that a particular e-mail has originated from a trusted site/party.
- **Spyware:** Malware that secretly monitors a user's computer activity.

- **Trojan:** Malware concealed within a genuine application which runs in the background along with the genuine application.
- **Backdoor:** A vulnerability intentionally left in the computer system/software by the designers.
- **Hacker:** A term used to describe a person who breaks into a computer system with the purpose of finding vulnerabilities, stealing, manipulating or destroying data/systems. Depending on the nature of activity being conducted, a hacker may be classified as an ethical hacker or a black hat hacker.
- **Virus:** A computer programme designed to make copies of itself and spread from one machine to another across the network.
- **Worm:** A worm is akin to a virus in the sense that it also replicates itself for spreading to other computers on the network. Whereas the virus almost always corrupts or modifies files on the targeted computer, the worm generally does not damage the targeted computer files but can cause harm by hogging bandwidth or opening secret backdoors for access to the machine/network.
- **Pen Testing:** Short form of penetration testing. It is the practice of testing a computer system to find vulnerabilities that can be exploited by cyber criminals.
- **Zero Day Vulnerability:** A zero day vulnerability is a flaw in the machine/network's operating system or application software which has not been fixed by the developer (patch for the vulnerability has not been released) and can be exploited by a hacker who is aware of it.

Fake news and Misinformation Campaigns: Availability of free information online, either in the form of news based apps and services or through messages forwarded via social media platforms also known as internet intermediaries, has given rise to the phenomena of fake news with often very serious and sometimes fatal consequences in the real world. The term "Fake News" in a sense is an oxymoron as news is something which is verifiable and in the public interest. Disinformation, a more serious form of misinformation refers to deliberately (often orchestrated) trying to confuse or manipulate persons by promulgation of dishonest information. The Cambridge

Analytica scandal consisting of the harvesting of Facebook profiles and thereafter bombarding vulnerable cross sections of the society with targeted ads to swing votes during an electoral process, is an example of disinformation. The reason for the rapid rise of fake news is due to little, or no regulation, of the content which is passed by the internet intermediaries coupled with end to end privacy between users afforded by almost all social media companies. The large numbers of digitally illiterate people, especially first time users of internet, promote faster spread of such hoaxes and misleading information with harmful effects in the real world.[40]

Pornography and Societal Degradation: The global porn industry is valued at a staggering $97 billion worldwide with almost 800 million porn pages available on the internet. Most of the porn is available for free with a pervasive culture of 'tube sites' which work on a model of 'try before you buy' and generate revenue based on the number of site visits or hits. There are numerous scholarly articles on the harmful impact of porn on individuals and society. The problem gets heightened when children who start using smartphones at young and tender ages, get free access to pornography and minors also get lured and enticed into 'child pornography'. A number of developing countries who have been largely conservative societies have often blamed the internet and online pornography for the 'loose morals' of present generation of youth, as well as increasing cases of rape and sexual assaults.

End to End Encryption: Most of the internet intermediary companies are presently providing end to end encryption between two or more parties when they talk, video call, chat and transfer documents between each other across different geographical locations. The advantage of an end to end encryption system is that only the user who has originated the message and the user who has received the message, are able to see the unencrypted version of the message. Everywhere in between, including at the internet intermediary server location, the message is in the encrypted form and cannot be converted back into unencrypted form. When the user first installs the chat application on his laptop or smartphone, a pair of public as well as private key gets generated. The public key is shared with the central server while the private key resides in the user individual laptop and smartphone itself. When a user desires to send a message to a recipient, he requests for the recipient's public key from the central server and encrypts the message using the same public key. This encrypted message is then transferred to the recipient's laptop or smartphone where it is decrypted using the private key of the recipient. Since the private keys remain on individual personal devices, the messages can only be decrypted at the individual user end. Though end to end encryption offers an extremely high level of privacy, but, when coupled with anonymity on the internet, it also poses a serious challenge for the law enforcement and national security agencies. A large number of anti-national activities happen on the internet making use of the anonymity, end to end encryption and global reach of the medium.

State Sponsored Mass Surveillance: The revelations of Edward Snowden in 2013 relating to the collaborative effort by a number of countries led by USA, to carry out mass surveillance of bulk internet traffic, took the whole world by storm. It was quite evident that personal information of a very large number of citizens of different nationalities was compromised as part of this global programme called 'Prism'[41] and that a large number of global ICT companies including Google and Facebook were actively participating in this programme. A number of court judgements recently have outlined how such activities may be undertaken keeping in mind both user rights, as well as national security considerations. In the case of Big brother watch and others v. the United Kingdom[42] concerning the bulk interception of communications, intelligence sharing with foreign governments and obtaining communication data from communication service providers, the European Court of Human Rights gave the following judgement on September 13, 2018:

- Bulk interception regime violated Article 8 of the European Convention on Human Rights (Right to respect for private and family life/communication).
- The regime of obtaining communication data from communication service providers also violated Article 8 of the convention.

- Both bulk interception regime and regime of obtaining communication data from communication service providers violated Article 10 (Freedom of expression) of the convention.
- The regime for sharing intelligence with foreign governments did not violate either Article 8 or Article 10 of the convention.

On May 25, 2018, the US Supreme court in a landmark judgement in the case of Carpenter V. United States,[43] ruled that authorities must obtain warrants in order to access mobile tower records, which can provide the accurate time bound location of a mobile phone user. Prior to this ruling, authorities could requisition mobile tower records without warrants by claiming that the records were required in connection with ongoing investigations. The ruling is bound to have ramifications on the way citizen's private data is collected by state agencies and introduce stricter procedures on collection and handling of person's private digital data.

Data Theft: Stealing or loss of data is one of the most common as well as serious cybersecurity risks at the present time. As more and more data is getting generated and swapped between multiple individuals, companies as well as government agencies, the chances of a data theft, are ever increasing. The largest data theft was that of Yahoo Inc. wherein three billion accounts got compromised. In 2018 alone, US accounted for 1244 data breaches with 446.5 million accounts compromised. In 2017, the US credit rating agency Equifax reported the loss of 145.5 million records including sensitive information like names, social security numbers, dates of birth, addresses, driving licence numbers etc. In 2019, Facebook admitted that 540 million user accounts were exposed on Amazon cloud server. Exchange of sensitive information for money is a booming crime industry and each loss or compromise of sensitive data is estimated to cost $150 on an average. The primary reason for loss of data is poor data security compliance by intermediaries, absent or weak laws and lack of cyber education and lax attitude on the part of the cyberspace user.

Individual Digital Privacy: Personal Individual Information (PII) of a person includes name, birthday, hometown, addresses, locations, interests, relationships, email addresses, photos, videos etc. A large number of cyberspace users routinely share their PII with a number of ICT companies, especially social media companies. Of late, the PIIs have been compromised, stolen, lost and exploited by individuals and companies, with no intimation and utter disregard for the individual digital privacy rights.

Individual digital privacy concerns have recently drawn the attention of governments and law makers the world over. The European Union's General Data Protection Regulations (GDPR) have been enforced since May 25, 2018. Under the GDPR, firms anywhere in the world that collect data on EU citizens, need to offer the user the option to see the information collected about them and to move or delete that information. Firms are also required to report any data breach within 72 hours of occurrence. The penalties for violating GDPR are also significant with maximum of $23.5 million or 4 per cent of firm's revenue, whichever is more.

Different countries have different takes on the onus of responsibility for protecting individual digital privacy. The Chinese approach to data privacy is different from that of the EU and US. While EU believes that data privacy is the responsibility of the user and the US believes that it is the responsibility of the tech firms who should police themselves, the Chinese believe that it is the government's responsibility to protect individual user's private data. The Chinese cybersecurity laws which were enforced in 2017, require Critical Information Infrastructure Operators (CIIOs) to store personal information and important data collected and generated, within China. It is also in the process of formulating rules for cross border transmission of personal Information and important data.

In India, the Justice B.N. Srikrishna committee submitted a draft data protection bill named the Personal Data Protection Bill, 2018 to the government on July 27, 2018. The draft bill calls for a comprehensive data protection laws to include data protection obligations, grounds for processing of personal data, rights of the data principle(confirmation, access, correction, data portability and right to be forgotten), various transparency and accountability measures and restrictions on cross border transfer of personal data. The bill is yet to be passed into law.

Since India presently lacks data privacy laws, the act of data compromise or data harvesting can be considered immoral and unethical but not illegal. Hence, users in India are presently unable to sue social media companies for data loss or compromise.

Fragmentation of the Internet:[44] There is a lot of concern lately regarding internet fragmentation or turning the global internet into loosely coupled islands of connectivity, based on territorial boundaries. The forefathers of the internet wanted a common artificial domain where each device could seamlessly connect with another, irrespective of their geographical location and brand of hardware or software, in order to exchange information and drive innovation. The drivers of internet fragmentation can be divided into three namely, technical reasons, governmental policies and commercial activities.

The technical fragmentation constitutes reasons for impeding the ability of different networks to fully interoperate and exchange data packets amongst each other. This could be because of difference arising due to network address translation, IPv4 and IPv6 incompatibility, routing corruption, firewall protection etc.

Governmental control and policies include: steps taken to block websites; social media accounts and other digital content; blocking user access to different types of content; restricting international connections; requirements to store and process data locally; making architectural changes to ensure that data flows within a given geographical area, etc.

Commercial fragmentation can be effected by making changes in inter organisational connectivity, throttling or blocking competitor's data and geo-blocking of content, etc.

There has recently been a rise in a number of countries moving away from a truly connected and homogeneous internet to a more domestic and regulated one. China has a significant different internet than the rest of the world and recently Russia and Iran have plans to disassociate themselves from the global internet ecosystem, with Russia testing its domestic internet in December 2019.[45]

Dark Web: The Dark Web is part of the internet which is not indexed by the search engines. As the name suggests, the Dark

Web is primarily used for transacting a large number of illicit and criminal activities. These activities range from sale of stolen IDs, documents, subscription accounts, etc. to sale of drugs, narcotics, guns and weapons etc. Some sites offer hired criminals and hackers for carrying out violent crimes as well undertaking DDOS attacks on networks and computers. Most of the financial transactions are carried out using crypto currencies like bitcoin. According to a recent survey 57 per cent of sites on Dark Web host illicit material and advertise criminal activity.[46]

Accessing the Dark Web requires an 'anonymising' browser caller Tor which routes a web page address through a number of proxy servers to make the IP address unidentifiable and extremely difficult to locate. The Dark Websites use the extension .onion in place of .com or .org, etc.

Law Enforcement Agencies (LEA) are improving their ability to track down the various web sites being operated on the Dark Web and recently a collaborative effort by three nations resulted in the shutdown of a popular Dark Net Site called Alpha Bay.

Cyber Crime: Cyber-crime has emerged as one of the fastest growing industries in the world with a global revenue of $1.5 trillion. Most of the cyber-crime revenue comes from illegal online market ($860 billion) and the online thefts and smuggling of trade secrets ($500 billion). Other major sources of revenue are data trading ($160 billion), crime-ware ($1.6 billion) and ransomware ($1 billion).[47]

Symantec Lab's *Internet Security Threat Report 2019,*[48] provides some interesting statistics, namely:

- In 2018, Microsoft Office files accounted for 48 per cent of all malicious email attachments, a steep rise from 5 per cent in 2017.
- India has a relatively safe malicious email rate of one in 772 as compared to one in 674 for USA and one in 255 for UK. It has a spam email rate of 50.9 per cent which is comparatively better than 57.5 per cent for US and 54.8 per cent for UK.
- US with 24.7 per cent tops the list of countries affected with mobile malwares followed by India with 23.6 per cent.

- US also tops the list of countries targeted by cyber groups with 255 attacks in 2018, followed by India with 128 targeted attacks.
- The cost of stolen IDs and fake passports and IDs on the Dark Web ranges from: $0.1 to 1.5 for stolen or fake ID; $15 to 25 for mobile phone online financial account; $1 to 35 for a ID/ Passport scan; $50 to 220 for fake health ID card; and $25 to 5000 for fake ID/driving licence, passport, etc.

In an online article published jointly by Cisco and Cybersecurity Ventures[49] (a leading cybersecurity firm), a number of important cybercrime statistics and trends were elucidated. Some of these are:

- Cybercrime is the fastest growing crime in the world with a projected global cost of $6 trillion by 2021, which is more than the cost of natural disasters or illegal drug trade in the entire world.
- By 2021, more than 70 per cent of all crypto currency worldwide will be used for illegal purposes. Presently, $76 billion worth of bitcoins are used for illegal transactions every year.
- Cybercrimes are grossly under reported. As per US Federal Bureau of Investigation (FBI) Internet Crime Complaint Centre (IC3), only about 10 to 12 per cent of total cybercrimes are actually reported.
- Data breaches have increased globally. The five major data breaches are: Yahoo (3 billion in 2013); Marriot (500 million from 2014-2018); Adult Friend Finder (412 million in 2016); My Space (360 million in 2016); and Under Armor (150 million in 2016).
- Hacks on crypto exchanges to steal crypto currencies is on the rise. The major bitcoin hacks are: Mt Gox (7,50,000 BTC in 2011); Bit Floor (24,000 BTC in 2012); Bit Stamp (19,000 BTC in 2015), Bitfinex (120,000 BTC in 2016). In 2018, crypto currencies worth a billion dollars were stolen from crypto exchanges.
- About 111 billion lines of software code is being written every year. This greatly increases the lists of vulnerabilities in the

cyberspace domain. It is estimated that by 2021, there will be one zero day exploit introduced every day, which is a sharp increase from one per week in 2015.

- The top five industries hacked in the past five years were health care, manufacturing, finance, government and transportation.
- Distributed Denial of service (DDoS) attacks are the most predominant as observed by internet service providers. These attacks utilise up to 25 per cent of the total internet traffic of a country, when the attack is underway. The report predicts that the number of DDoS attacks will double from 2017 to 14.5 million attacks in 2022.
- Hacking tools and sophisticated kits for launching cyber-attacks, identity thefts, malware and ransomware attacks are available on the Dark Web at prices as low as one dollar. This makes the cost of entry almost negligible and would motivate a large number of people to resort to cyber-crime.
- Ransomware is the fastest growing cyber-crime in the world with the US Department of Justice (DOJ) terming it as the "New Business Model" for cyber criminals. Losses due to ransomware attacks globally in 2021 are projected to be $20 billion, which is an exponential rise from 2015 ($325 million) and 2017 ($5 billion).
- More than 90 per cent of cyber hacks and identity frauds originate as phishing attacks (email meant to lure the victim into clicking a malicious code or link).
- Crypto jacking is a new entrant into the world of cyber crime, which is gaining popularity. In crypto jacking hackers use the target computer's processing power to mine for crypto currencies. The problem has reached a stage wherein Google has decided to ban all extensions on its Chrome browser that lead to crypto currency mining.
- With the coming of IoT, the number of internet connected wearable devices will increase form 310 million (in 2017) to 500 million in 2021.
- A large number of persons are now vulnerable to cyber-attacks on their wirelessly connected, digitally monitored Implantable Medical Devices (IMD) like defibrillators, pacemakers, insulin pumps, ear tubes, etc.

Cyber-Terrorism: It can be defined as the use of cyberspace to conduct violent attacks which are aimed at causing harm to the user and leverage fear, threat and intimidation to achieve ideological or political advantages.

The internet has always been used by non state actors especially terrorist organisations like Al-Qaeda and ISIS. Initially the internet was used for secret communications, recruitment and ideological propaganda but morphed into more violent forms like spread of hate and fear, by the circulation of highly objectionable hate speeches and videos of gruesome acts of killings and violence.

The use of cyberspace to carry out more severe forms of attacks on individuals, governmental agencies and financial and other infrastructure like oil pipelines, refineries and power grids is the latest form of cyber terrorism, that the world is facing today.

There are numerous examples of cyber terror attacks. The cyber group Anonymous regularly carries out DDOS attacks on individuals, agencies and other groups, whom it considers working against them. In April 2007, Estonia witnessed a number of DDOS attacks which literally brought the country to a standstill and affected most of its online services, including banking and telecommunications. The attacks are believed to be carried out by Russia because of the removal of a WWII bronze statue of a soviet soldier from the capital Tallinn. On August 15, 2012, the computer network of Saudi oil giant Aramco was affected by a self-replicating virus which affected more than 30,000 computers and brought operations to a near standstill for weeks. The *Not Petya* and *WannaCry* ransomware attacks are also recent examples of cyber terrorism.

An Introduction to Cyber-War: Concepts and Techniques

Information Warfare (IW): The concept of information warfare is not new to mankind and has been exploited over the years by different civilisations across the world. In the *Mahabharatha*, the news of the death of the elephant named *Ashwathamma* was conveyed by *Yudhishtar* to *Dronacharya* in such a manner that he believed that his son, of the same name, was dead, which made him give up arms and subsequently get killed on the battlefield.

IW can be defined as "a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries".[50]

Martin C. Libicki,[51] an expert on Information warfare proposed various forms of IW, namely:

- Command & Control Warfare (C2W)
- Intelligence Based Warfare (IBW)
- Electronic Warfare (EW)
- Psychological Operations (PSYOPS)
- Hacker war-software based attack on information systems
- Information Economic Warfare (IEW) or war via the control of information trade
- Cyber warfare (combat in virtual realm)

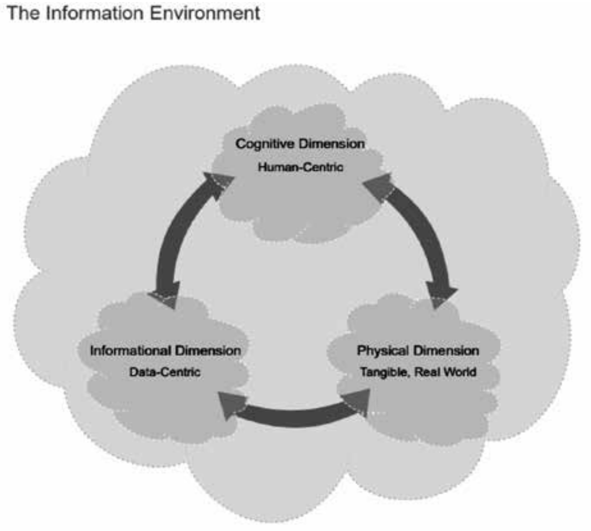
Information Operations (IO): US Joint publication 3-13[52] on IO defines it as:

> The integrated employment, during military operations, of Information Related Capabilities (IRCs) in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own.

The Information Environment (IE) is defined as "The aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information". The IE consists of three inter related dimensions of physical, information and cognitive which continuously interact with individuals, organisations and systems. The physical dimension is composed of Command and Control (C2) systems, key decision makers and supporting infrastructure of physical platforms (human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablets, computers, etc.) and communication networks. The information dimension deals with collection, processing, storage, dissemination and protection of information while the cognitive dimension is the minds of the persons who transmit, receive, respond or act on this information.

The Target Audience (TA) is the individual or group which is selected for conduct of IO. IRCs are tools, techniques and activities which are used by the TA to collect, process or disseminate information. The aim of IO is to shape the TA's conditions, capabilities, situational awareness and ability to make and share timely and informed decisions in order to contribute favourably towards the desired end state.

Cyberspace Operations (CO): US Joint Publication 3-12[53] defines cyberspace operations as, "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."



Source: US Joint Publication 3-13.

As mentioned earlier, cyberspace consists of three layers namely, physical, logical and cyber persona. The cyberspace is a subset of the Information Environment. The Operational Environment (OE) is the sum total of conditions, circumstances and influences that affect the employment of capabilities and impacts the decisions of the commander responsible for conducting CO.

CO can be divided into three cyberspace missions: Offensive Cyberspace Operations (OCO); Defensive Cyberspace Operations

(DCO); and Department of Defence Information Network (DODIN) Cyberspace Operations. OCO are CO missions intended to project power in, and through, foreign cyberspace. DCO missions are executed to defend the DODIN or other critical cyberspace from active threats. The DODIN operations mission includes operational actions taken to secure, configure, operate, extend, maintain and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN.

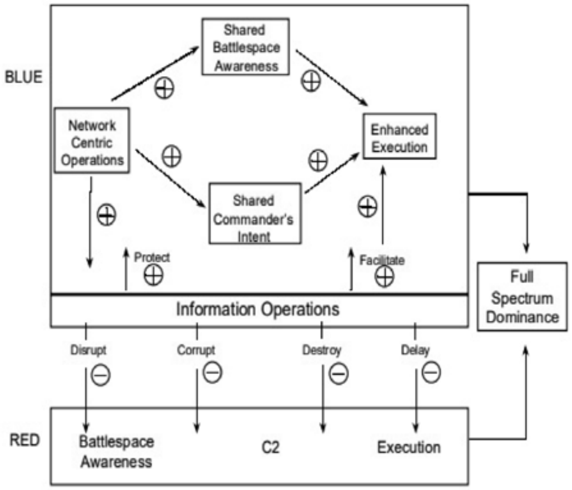
Network Centric Warfare (NCW): NCW can be defined as an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronisation. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.[54]

The information age is making decision making complex due to generation of vast quantities of information in real, or near real time, over geographically spread out locations. Thus, though the information load has exponentially increased, the time and space domain have shrunk considerably. Therefore, responsiveness and agility to decide, post processing the entire information is becoming a critical attribute in deciding the success or failure, of any organisation in the Information age.

Information superiority is a state that is achieved when a competitive advantage is derived from the ability to exploit a superior information position. Metcalfe's law describes the potential value of a network and states that as the number of nodes in a network increase linearly, the associated '*value*' or '*effectiveness*' of the network increases exponentially as the square of the number of nodes in the network. In other words, the effectiveness of a networked system with large number of nodes is exponentially greater when compared to a network, which has considerably lesser number of nodes. Thus, networking of all components of an organisation or force will result in information superiority over an adversary, with lesser number of networked nodes or conversely, by destroying or reducing the number of nodes of an adversary's network will exponentially reduce his information superiority.

In the military domain, Information Superiority will translate into "the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[55] It implies that military combat power can be greatly enhanced by networking sensors, decision makers and shooters to achieve shared awareness, increased speed of command, heightened tempo of operations, greater lethality, increased survivability and a high degree of self-synchronisation. The same results in full spectrum domination enabled by information superiority.

Full Spectrum Domination Enabled by Information Superiority



Source: Network Centric Warfare[56]

Common Interception Techniques: There are a large number of interception techniques available for monitoring the data being generated on the network. The data generated by a system can be at rest (residing on the machine in a specified memory location) or in transit (moving from one node to another). Details of some common interception techniques are given in subsequent paragraphs.

- **Data at Rest:** The data at rest can be compromised by activating malwares on the host machine which is capable of copying resident data and thereafter transmitting it to servers/machines of hackers. Some of the common data stealing methods are password crackers, Trojan horses, keyboard loggers, phishing attacks, backdoor attacks and various spyware programmes.

- **Data in Transit:** Interception of data in transit can be carried out in multiple ways and would depend on whether the last mile connectivity was wireless (using a Wi-Fi router or mobile phone), or wired (using OFC or coaxial cable for connecting directly to the computer). In addition, all Internet Service Providers are mandated to keep detailed logs of internet, voice calls and mobile tower access by customers for use by law enforcement agencies. In 2013, Edward Snowden revealed that mass surveillance of internet was being carried out by the US, Australia and Canada (member countries of Five Eyes pact), using a global surveillance system called PRISM. There were also revelations about an automated malware injecting system called TURBINE.

Common Disruption Techniques: DDOS is one of the most prevalent means of disrupting services on a target computer or server. In addition, there are innumerable malwares available for partially, temporarily or permanently destroying data or equipment. *Stuxnet* is a cyber weapon which targets Supervisory Control and Data Acquisition (SCADA) systems, used to control complex infrastructure and industrial processes. In 2010, it exploited zero day vulnerabilities of Windows operating system to target centrifuges running in Iran's nuclear facility, causing equipment failure which led to subsequent closure of facility.

Cyberspace Doctrines of US, China, Russia and India

Cyberspace Doctrine of US: The US released its National Defence Strategy[57] in 2018 at a time when the world was witnessing increasing trade wars between US and China and an assertive role being played by US in the Asia Pacific region and West Asia. US acknowledged that it was emerging from a period of 'Strategic atrophy' with its competitive military advantage eroding. There was increased global disorder creating a security environment which was highly complex and volatile. Inter-state strategic competition rather than terrorism, is the US primary national security concern.

The US regards China, Russia, North Korea and Iran as key nations responsible for the current turmoil in global world order and geo-strategic environment. It considers China to be a strategic competitor that is adopting predatory economic policies while "militarising" South China sea. Russia has violated the borders of neighbouring nations and "pursues veto powers" over their economic, diplomatic and security decisions. North Korea's outlaw actions and "reckless rhetoric" continues unabated while Iran continues to "sow violence" and remains the most significant challenge to Middle East stability.

The US acknowledges that they are presently facing more lethal and disruptive battlefield where each domain (air, land, sea, space and cyberspace), is keenly contested. It believes that the technologies of advance computing, 'big data' analysis, artificial intelligence, autonomy, robotics, directed energy, hyper-sonics and bio-technology will be the key enablers for winning the wars of the future.

The US strategic objectives outlined in the National Defence Strategy are first, to be strategically predictable but operationally unpredictable; second, to integrate with other US inter agencies; third, to counter coercion and subversion and lastly, to foster a competitive mindset. To achieve these strategic objectives, US will build a more capable and lethal joint military force, strengthen existing alliances and foster new ones and make the existing Department of Defence's business practices more efficient and affordable.

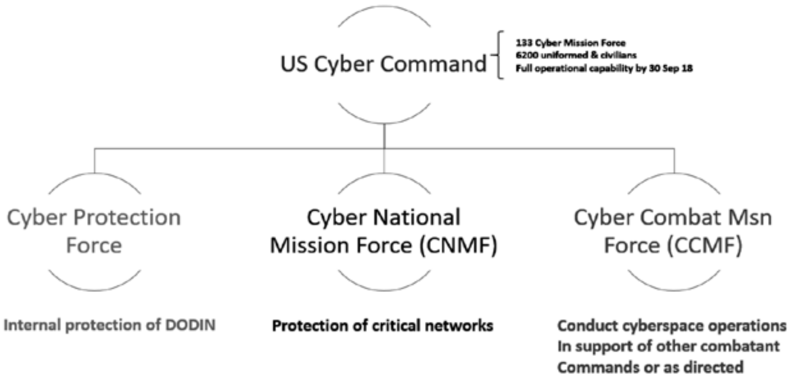
In September 2018, the US DoD released its cyber strategy[58] after a gap of three years. It acknowledged that China and Russia are their long term strategic competitors. The strategy acknowledges that China is eroding the US military's competitive edge as well as the nation's economic vitality by consistently "exfiltrating" sensitive information from US public and private sector institutions. Russia, on the other hand has employed cyber enabled information operations to influence US population and challenge its democratic processes.

The US DoD strategy against cyber-attacks would be to expose, disrupt and degrade those activities which threaten US interests. To ensure the above, the DoD will enhance the military's capabilities to fight and win wars in any domain, including cyberspace. Second, the DoD will pre-empt, defeat or deter malicious cyber activity targeting US critical infrastructure that could cause a significant cyber incident; and lastly, the DoD will cooperate and collaborate with allies and partners to strengthen cyber capacity, expand combined cyberspace operations and increase bi-directional information sharing.

The US DoD has also acknowledged that its Joint Force will employ offensive cyber capabilities and innovative concepts, that will enable cyberspace operations across the full spectrum of conflict.

The US has also moved towards a policy of 'name and shame' or attributability in cyberspace as a means towards dissuasion. Towards that end, in May 2014, it indicted five Chinese People's Liberation Army (PLA) personnel of Unit 61398,[59] for hacking into American companies, including Westinghouse, United States Steel and Alcoa. This was followed again by the indictment of three Chinese hackers on November 27, 2017 for Intellectual Property theft by hacking into three US corporations.[60] On July 13, 2018, 12 Russian intelligence operatives were indicted by US Justice Department for the 2016 hacks of the Democratic National Committee (DNC). On December 20, 2018, the US FBI indicted[61] two Chinese men who are part of Chinese government's Advance Persistent Threat (APT)-10 group, of conspiracy to commit computer intrusion, conspiracy to commit wire fraud and aggravated identity theft against more than 45 companies through massive hacking campaigns, from 2016 to 2018. On February 10, 2020, the US Attorney General indicted four members of Chinese military for hacking into US company Equifax's computer networks, maintaining unauthorised access and stealing sensitive information.[62]

The US Joint Publication 3-12[63] on "Cyberspace Operations" enumerates three cyberspace missions for DoD namely: Offensive Cyberspace Operations; Defensive Cyberspace operations and maintenance; and security of DoD Information Network (DODIN). On May 4, 2018, the US Cyber Command became the tenth full-fledged command with fully operational capabilities. The US Cyber Command comprises of 6200 uniformed and civilian personnel and is divided into 133 cyber mission forces which are grouped into Cyber Protection Force, Cyber National Mission Force (CNMF) and Cyber Combat Mission Force (CCMF).


US Cyber Command
133 Cyber Mission Force
6200 uniformed & civilians
Full operational capability by 30 Sep 18
Cyber Protection Force
Cyber National Mission Force (CNMF)
Cyber Combat Msn Force (CCMF)
Internal protection of DODIN
Protection of critical networks
Conduct cyberspace operations In support of other combatant Commands or as directed

Cyberspace Doctrine of China: China, in the last decade or so, has embarked on an ambitious programme to modernise its defence forces for "winning local wars under conditions of informationisation".[64] The start of China's 13th Five Year Plan in 2016 witnessed unprecedented restructuring of the People's Liberation Army (PLA) to ensure that it meets its ambitious goals to fight and win integrated, joint wars in all domains of air, land, sea, space, cyberspace and electromagnetic.[65]

The initial military strategy formulated in 1949 was the strategy of "Active Defence" which primarily implied that "We will not attack unless we are attacked, but we will surely counter-attack if attacked". This was suitably modified to "Winning local wars under hi-tech conditions" in 1993 and to "winning local wars under conditions of informationisation" in 2004. A doctrinal concept of integrating Computer Network Operations (CNO) and EW in order to fight in the 'informationised' domain has been introduced by China and forms part of its 4th General Staff Department named "Integrated Network and Electronic Warfare (INEW)".[66]

In May 2015, China released its white paper on "China's Military Strategy".[67] It emphasised that, "Profound changes" are taking place in "balance of power, global governance structure, Asia-Pacific geostrategic landscape, and international competition in the economic, scientific and technological, and military fields."

The White Paper stated that the world is moving towards multi polarity, economic globalisation and information society. In the Asia-Pacific region, the US is carrying out a "rebalancing" strategy and enhancing its military presence in the area. Japan is "overhauling" its military and security policies, which is of grave concern to the countries in the region. Also, some countries are interfering and taking provocative measures in the South China Sea region and thus posing a challenge to China's territorial sovereignty and maritime rights. Instability and uncertainty are ongoing in the Korean peninsula and North East Asia. In addition, anti-China forces are attempting a "colour revolution" coupled with dissenting voices of "East Turkistan independence" and "Tibet Independence". In the field of "Revolution in Military Affairs (RMA)", rapid developments are taking place in areas of long range, precise, smart, stealthy and unmanned weapons and equipment with outer space and cyberspace gaining "Commanding heights" in strategic competition.

The mission and strategic task given to the armed forces is to be acutely aware of the rapidly developing challenges in the security domain, seize strategic initiative in military competition, actively participate in regional and international security cooperation and effectively secure China's overseas interests. The armed forces will be in a continuous state of "Preparation of Military Struggle (PMS)" and amalgamate information dominance, precision strikes and joint operations, to fight by the principle of "You fight Your way and I fight My Way". Force development in critical security domains of seas and oceans, outer space, cyberspace and nuclear forces will be undertaken in line with the national defence strategy.

In December 2016, China released its National Cyberspace Security Strategy.[68] The strategy outlines that the widespread use of IT and cyberspace has resulted in economic and social prosperity but at the same time introduced new risks and challenges. Thus, maintaining China's cyber security is crucial for building a prosperous civil society, deepening reforms, improving state of law and order and managing the overall strategy of the communist party.

The strategy acknowledges that cyberspace has become an important domain like the air, sea, land and space and thus the concept of national sovereignty also extends to cyberspace. China has identified a number of factors that are challenging its cyberspace domain. First is the illegal use of cyberspace to interfere in the internal affairs, attacking political systems, inciting social unrest and carrying out large scale monitoring of network traffic. Second, increasing susceptibility of critical infrastructure to debilitating cyber-attacks. Third, erosion of morality, ideology, moral values and culture through internet rumours, decadent culture & obscenity, violence and superstition. Fourth, the use of cyberspace to fuel terrorism and illegal crime and lastly, the rising international competition in cyberspace with nations competing for controlling strategic cyberspace resources, rule making powers have intensified the cyberspace arms race.

China has set the following goals for achieving in cyberspace: First, use of cyberspace for peace by curbing IT abuse, controlling the global cyberspace arms race and preventing conflicts in cyberspace. Second, ensuring security of cyberspace by effectively controlling network security risks, having a national network security assurance system, use of safe core technical equipment, having an adequate cyber skilled technical workforce and ensuring a high level of cyber hygiene standard in civil society. Third, promoting openness by ensuring that IT standards, policies and markets are open and transparent, with no digital divide amongst nations. Fourth, carrying out closer cooperation with all nations for technology exchange and combating cyber terrorism and cyber-crime and lastly ensuring that user rights, expressions and privacy are effectively protected and human rights respected.

China will govern its cyberspace on four principles. First, maintaining cyber sovereignty by ensuring that domestic information systems and resources are protected from intrusion, interference, attack and destruction. The state will guarantee the legitimate rights and interest of citizens in cyberspace. Second, promoting peaceful use of cyberspace. Third, governing cyberspace as per rule of law and lastly coordinating network security and development.

China has laid out nine strategic tasks to be achieved as part of its cyberspace strategy. First, to firmly defend its cyberspace sovereignty. Secondly, safeguard national security by preventing, stopping and punishing anyone using internet for anti-national activities. Third, protecting national critical information infrastructure especially pertaining to energy, finance, transportation, education, scientific research, water conservation, industrial manufacturing, medical and healthcare, social security, public utility, state agencies and important internet application systems. Fourth, strengthening and developing network culture through content construction projects aimed at cultivating national core values, promoting cultural exchange, building a civilised and honest network environment etc. Fifth, combating cyber terror and illegal crime. Sixth, improving network governance system. Seventh, consolidating network security. Eighth, improving cyberspace protection abilities and lastly strengthening international cooperation in cyberspace.

Cyberspace Doctrine of Russia: Russia released its ‘National Security Strategy for 2020’ on May 12, 2009.[69] The policy states that Russia is pursuing a state policy of “National Defence, state and social security and stable development”. The world is on the path of globalisation that is characterised by a high degree of dynamism and interdependence of events. The inadequacy of current global and regional architecture, which is centred around NATO, coupled with the inadequacies of legal instruments and mechanisms is creating an ever increasing threat to international security.

The challenges facing the Russian Federation arise from recurrent one sided use of force in international relations, threats of proliferation of weapons of mass destruction and their use by terrorists and illicit activity in the cybernetic and biological domain. The global information struggle would intensify with the global demographic situation and environmental problems becoming more acute.

Post the National Security Doctrine of 2009, Russia released a number of other doctrines in quick succession. The Military

Doctrine was released in 2010, which was followed by a second Military Doctrine in 2014 and a second National Security Strategy document on December 31, 2015. The Doctrine on Information Security was released in December 2016. The National Security Strategy of 2009 was invalidated vide the National Security Strategy document released on December 31, 2015.

The Military Doctrine of the Russian Federation was released on December 25, 2014.[70] The doctrine acknowledges that the military risks and threats are migrating to the "information space and internal sphere" of the Russian Federation. The major external military threats to Russia include the NATO build up and the moving of its military infrastructure near to the Russian Federation borders; deployment of strategic Missile Defence Systems; weaponisation of space; proliferation of Weapons of Mass Destruction (WMD); missiles and missile technology; the growing threat of global terrorism; expansion of trans national organised crime and; use of ICT for military-politico purposes.

The doctrine refers to emerging use of high precision hypersonic weapons, electronic warfare systems, other weapons based on new physical principles that are comparable to nuclear weapons, use of information and control systems, drones and autonomous marine vehicles, guided robotic weapons and military equipment. To enhance the effectiveness of its defence forces, the doctrine outlines a host of measures including enhancing the capacity and means of IW as well as enhancing the integrated net centricity of the entire force into a single information field.

The Russian National Security Strategy of 2015[71] has once again referred to the use of ICT to achieve geo-political objectives including manipulating public awareness and falsifying history and emergence of new types of unlawful activities, especially those involving the utilisation of "informational, communications and high technology". An important aspect of the new security strategy is the emphasis on educating school children "as responsible citizens of Russia on the basis of traditional Russian spiritual-moral and cultural-historic values", which could be because of the perceived degradation of values and societal norms primarily due to large scale proliferation of ICT and the attempts by adversaries to subvert the populace by resorting to psychological tools.

Russia released its doctrine on information security on December 5, 2016.[72] The doctrine emphasises that a large number of countries are building up their IT capacities for military purposes and a host of intelligence agencies are using information and psychological tools for destabilising the internal political and social fabric of various states. Several non-state actors like religious, ethnic, human rights organisations, other organisations and separatist groups are also actively engaged in such activities.

It also underlined that due to heavy reliance of domestic industry on foreign IT equipment and software, the socio-economic development of the Russian Federation becomes dependant on the geo-political interests of foreign countries. The absence of international legal norms in cyberspace as well as the mechanism for their implementation, makes it difficult to "create an international information security system designed to achieve strategic stability and equitable strategic partnership".

The strategy identifies five key areas to ensure information security in the field of national defence. First, ensuring strategic deterrence and preventing military conflicts resulting from use of IT. Second, upgrading the information systems of Russian Armed Forces. Third, forecasting, identifying and assessing information threats. Fourth, promoting the interests of the Russian Federation and allies in information sphere and lastly, taking appropriate steps to counter adversaries information and psychological actions.

Timothy Thomas in an article on Russia's IW strategy[73] argues that Russia broadly divides IW into two major groups i.e. information-technical and information-psychological. He further states that Russia is acutely aware of the important role being played by cyber and the asymmetrical results which can be achieved by undertaking suitable information operations. Also, due to the country's emphasis on maths and science education, the quality of Russian code developers and hackers is extremely high compared with code developers and hackers in other countries. Kar Flook in an article[74] points out that some hackers have been offered the option of working for the Russian government instead of undergoing a prison sentence.

Michael Connell and Sarah Vogler in their article[75] on Russian cyber warfare strategy have stated that offensive cyber warfare is playing a greater role in Russia's conventional military operations and will play a decisive role in its strategic deterrence framework. According to James Clapper, the Director of US National Intelligence, "Russia's cyber capabilities are highly advanced and Moscow has demonstrated a willingness to employ offensive cyber in situations other than war to affect political and economic outcomes in neighbouring states and to deter its adversaries". The Georgia and Ukrainian conflict provided Russia with an opportunity to refine its cyber warfare procedures and techniques and at the same time demonstrated its capabilities to the world. Hacktivists and cyber-criminal syndicates are the main actors in Russian offensive cyber operations primarily because of their anonymity and non attributability characteristics.

Cyberspace Doctrine of India: As per data released by Telecom Regulatory Authority of India (TRAI),[76] as of May 31, 2017, India had 1.1 billion telephone subscribers (the 2nd highest in world), 241 million Facebook users (highest in world), 1.15 billion digital IDs (largest national ID programme) and 463 million internet users (2nd highest in the world). Post demonetisation, India has witnessed a surge in digital financial transactions with the digital economy on track to grow from $270 billion to around one trillion dollars by 2024.[77] On January 5, 2018, the government of India informed the Parliament that cyber-crime cases registered in India have gone up from 9,622 in 2014 to 12,317 in 2016.[78]

The Indian government has taken a number of initiatives to improve the cyber security posture of the country. The ITU publishes a yearly Global Cyber Security Index[79] as a measure of the commitment of countries to cyber security. The assessment is carried out along five verticals, namely legal, technical, organisational, capacity building and cooperation, which is then aggregated to arrive at the overall score and global ranking of each country. The Global Cyber Security Index of 2017 featured 134 countries with India at 23.

The National Cyber Security Policy (NCSP)[80] was released in 2013. This lays down the vision (for building a secure and resilient cyberspace for citizens, businesses and government) and strategic direction to implement a strong cyber security enabled digital environment in the country. In 2014, the government launched the *Digital India* platform to transform India into a digitally empowered society. The platform has nine pillars. These are broadband highway; universal access to mobile connectivity; public internet access programme; e-governance; e-*Kranti* – electronic delivery of services; information for all; electronics manufacturing; IT for jobs and; early harvest programmes.

The NCSP acknowledges that IT is one of the major growth catalysts for the Indian economy and positively influences the lives of the populace by contributing to a host of socio-political parameters like employment, standard of living, diversity, etc. The essence of a secure cyberspace is the protection of information infrastructure and preservation of its confidentiality, integrity and availability. The policy lists out 14 objectives. Key among these are :creation of a secure cyber eco-system; creation of an assurance framework; strengthening the regulatory framework; creating National and Sectoral Computer Emergency Response Teams (CERT); establishment of a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC); creating a workforce of 5,00,000 professionals; and enhancing global cooperation for effective security of cyberspace.

The National CERT-In was made operational in January 2014. It has been designated as the national agency for undertaking a number of cyber security functions under the IT Amendment Act 2008. The NCIIPC was also operationalised in January 2014 and designated as national nodal agency in respect of critical information infrastructure protection. Transport, power and energy, telecom, government, banking, finance services & insurance and strategic public enterprises have been designated as critical infrastructure.

Headquarters Integrated Defence Staff (IDS), Ministry of Defence (MoD) released the joint doctrine of the Indian Armed Forces in April 2017.[81] The doctrine enumerates four national security objectives. First, maintenance of a credible deterrence capability to safeguard national interest. Second, ensure defence of national territory, air space, maritime zones including our trade routes and cyberspace. Third, to maintain a secure internal environment to guard against threats to our unity and development and lastly, to expand and strengthen 'constructive engagement' with other nations. Five National Military Objectives (NMO) have been outlined in the doctrine. First, to prevent war through strategic and conventional deterrence across the full spectrum of military conflict. Second, prosecute military operations to defend territorial integrity and ensure a favourable end state during war to achieve stated/implied political objective(s). Third, provide assistance to ensure internal security, when asked. Fourth, render Humanitarian Assistance and Disaster Relief (HADR), aid to civil authorities and international peacekeeping, when called upon to do so and lastly, have required degree of self-sufficiency in defence equipment and technology through indigenisation to achieve desired degree of technical independence by 2035.

The doctrine states that although conflict and "war for territory" are diminishing worldwide, they continue to remain relevant in the Indian context due to disputed borders. Strategic interests along northern, western and eastern borders and sensitivities along Line of Control (LoC) and Line of Actual Control (LAC) need to be defended adequately. It also acknowledges that radicalisation of youth by suspected social media platforms poses a contemporary challenge to national security and the management of the digital environment, which has "the ability to manage conflicts through social media", should be given high priority in the national security calculus.

The doctrine dwells on the four levels of war namely: political/ grand strategy; military strategy; operational; and tactical. The operational level links military strategy to tactics and employs land, air, maritime, cyberspace, space and special forces to jointly deliver a range of effects, that contribute towards success in battle. The world is currently witnessing hybrid war, which is a conflict characterised by the blurring of the lines between war and politics, combatants and civilians with chaos, psychological and media warfare, cyber warfare, economic warfare, etc. as important constituents.

The guiding philosophy of war fighting strategy would be "undertaking 'Integrated Theatre Battle' with an operationally adaptable force, to ensure decisive victory in a network centric environment across the entire spectrum of conflict in varied geographical domains".

The doctrine defines cyber power as "the ability to use cyberspace freely and securely gain an advantage over the adversary while denying the same to him in various operational environments, and by applying the instruments of National Power". It acknowledges the role of IW (including cyberspace), space and special operations in support of military operations. It states that the future wars are likely to be fought in the triad of space, cyber and special operations and steps have been initiated for establishment of a Defence Cyber Agency, Defence Space Agency and Special Operations Division. As part of the military's pursuit of capacity building for NCW, the recently launched integrated Defence Communication Network (DCN) will enable all stakeholders to share situational awareness for faster decision making. The Defence Information Assurance & Research Agency (DIARA) is the nodal agency dealing with all cyber security needs of the tri services and MoD. Coordination between the various agencies dealing with cyber, is ensured by the National Security Council Secretariat (NSCS) through National Cyber Coordination Centre.

Important Cyberspace Legislations

European Union (EU) General Data Protection Regulation: The EU GDPR[82] was approved by the EU parliament on April 14, 2016 and came into force with effect from May 25, 2018. The GDPR has replaced the Data Protection Directive 95/46/EC and is viewed as a watershed document for protecting and empowering citizen's data privacy.

The regulation designates data protection as a fundamental right and aims to ensure a high level of data protection in spite of its increased generation and exchange. One of the biggest changes in the GDPR is its extended jurisdiction. The GDPR is applicable to all companies processing the personal data of EU citizens irrespective of their geographical location (it could be within or outside EU). There has been an exponential increase in penalties with maximum fine that can be imposed for serious infringements of GDPR pegged at four per cent of the annual global turnover or €20 million (whichever is greater). The user consent for data use must be "clear and distinguishable from other matters and provided in an intelligible and easy assessable form, using clear and plain language". The purpose for data processing must be attached to the consent and it must be simple for the user to withdraw consent.

Another important aspect of GDPR is "Breach Notification". Under this, Data Processors are required to notify member states, customers and controllers[83] of the breach "without undue delay" and within 72 hours of first having becoming aware of the breach. The user has the right to ask the data controller whether their personal data is being processed or not, where and for what purpose. Furthermore, the controller shall provide copy of personal data in electronic format, free of charge to the user. Right to be Forgotten also known as "Data erasure" entitles the user to have the controller erase his/her personal data and stop its further distribution and processing. However, this right requires the controller to compare the user's "right" with "the public interest in the availability of data". Data portability is another new addition to GDPR. In this, the user can receive their personal data from one controller and thereafter send it to another.

The Federal Information Security Management Act (FISMA) of 2002: The FISMA[84] act of US government also known as Public Law 107-347 is meant to manage and promote e-government services as well as establish a broad framework of measures required to make these services more accessible to the general public. It establishes a set of best practices (guidelines and security standards) that all federal agencies and private companies dealing with the federal government have to follow. The act is considered one of the most important regulations dealing with data security. In April 2010, the Office of Management and Budget (OMB) released a set of guidelines which enable federal agencies to provide real time inputs to FISMA auditors for continuous compliance monitoring.

The FISMA implementation project was established in January 2003 to lay down key security standards and guidelines required for FISMA compliance. The National Institute of Standards and Technology (NIST) played a key role in this and a number of documents to include FIPS 199, FIPS 200 and the NIST 800 series were published.

Some of the major FISMA requirements are as under:

- **Information System Inventory:** All agencies including private companies working with federal agencies must have an updated inventory of all IT assets including the physical and logical interconnection between the various information systems as well as other systems within the network.
- **Risk Categorisation:** FIPS 199 (Standards for Security Classification of Federal Information and Information Systems) defines the risk levels of various information and information systems. All organisations have to classify their information and information systems as per FIPS 199 classification so that all sensitive information and information systems are provided with the authorised level of security.
- **System Security Plan:** A detailed security plan containing details of various security controls, security policies and contingencies has to be maintained by all organisations. This System Security Plan needs to be regularly practiced and updated in order to stay relevant and efficient based on latest detection of vulnerabilities and procedural lapses observed in the system over a period of time.
- **Security Controls:** NIST SP 800-53 gives an extensive list of suggested security controls for FISMA compliance. Agencies are not required to implement all the controls but only those that are relevant to their organisation. Once the controls have been selected, the System Security Plan needs to be updated and practiced to ensure that necessary security systems based on risk category of information and information systems are in place.
- **Risk Assessment:** NIST SP 800 – 30 gives detailed guidelines for the conduct of risk assessment by organisations. The risk assessment needs to be conducted at three levels i.e. at the organisational, business process and information system level in order to holistically identify the cumulative risks across the entire information flow cycle.

- **Certification and Accreditation:** FISMA mandates programme officials and agency heads to conduct annual security reviews. FISMA Certification and Accreditation (C&A) is carried out over four phases which are: initiation and planning; certification; accreditation; and continuous monitoring.

China's Cyber Security Laws: The cyber security law of the People's Republic of China[85] also known as China's Internet Security law was enacted by the Standing Committee of the National People's Congress on November 7, 2016 and implemented with effect from June 1, 2017.

The cyber security law has been divided into seven chapters and 79 articles. A complete chapter (Chapter 6) has been devoted to legal responsibilities and gives details of fines and punishments for infringement of various articles of the laws.

Article 1 of the law proclaims that the law has been formulated in order to "ensure cyber security; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organisations; and promote the healthy development of the informatisation of the economy and society."

Article 9 of the law states that apart from following laws and administrative regulations, Network Operators need to respect "social morality", accept "supervision" from the government and public and bear social responsibility.

Chapter III which deals with Network Operating Security gives details of the various duties of network operators to include formulation of the internal security management system and operating rules, adopting necessary technical measures to prevent cyber-attacks, provision to store network logs for minimum period of six months, methods to monitor and record network operational statuses and comply with other provisions of state given from time to time.

Article 23 of Chapter II states that critical network equipment and specialised cyber security products shall follow national standards and will be certified by a qualified establishment or get security inspection done prior to installation. Network operators are also mandated to formulate emergency response plans for various cyber security contingencies like cyber-attack and network intrusions.

China has a wide ranging and open ended definition of a Critical Information Infrastructure which includes:

> … public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which – if destroyed, suffering a loss of function, or experiencing leakage of data – might seriously endanger national security, national welfare, the people's livelihood, or the public interest.

Thus, almost everything dealing with cyberspace can be categorised as "Critical Information Infrastructure".

The Critical Information Infrastructure operators have to perform additional security protection duties apart from the duties being performed by network operators. These include: Setting up of specialised security management bodies; conducting security background checks on personnel employed in critical positions; conducting disaster recovery backup of critical systems and databases; and periodically organising emergency response drills. The Critical Information Infrastructure operators also undergo a national security review organised by State Cyber security and the informatisation department and relevant departments of the State council.

Article 37 mandates that all data generated by Critical Information Infrastructure operators during operations within the Chinese territory, will be stored within China only.

Chapter IV on Network Information Security lays strong emphasis on privacy of private user data and asks network operators not to gather personal data in excess of the level of services they provide and that only after obtaining due consent of the user. In addition, the network operators will take all technical and other measures necessary to ensure the security of personal information and prevent it from leakages, destruction or loss.

Information Technology Act 2000 & IT (Amendment) Act 2008: The Information Technology Act – 2000,[86] also known as ITA-2000 or IT Act was enacted by the Indian Parliament on June 9, 2000 and is the principle act dealing with cyber-crime and e-commerce in India. The Act comprises of 94 sections compiled into 13 chapters and four schedules.

Under the IT Act, legal recognition was accorded to electronic records, digital signatures and their use in government and its agencies. Rules and procedures regarding appointment of a Controller of Certifying Agencies as well issuing of digital signatures are included in the act. On the cyber-crime front, penalties pertaining to tampering with computer source documents, hacking of computer systems and networks, publication of obscene information in electronic format have been elucidated. In addition, the Act gives directions for the establishment of a Cyber Appellate Tribunal for dispute resolution and powers to police officers, not below the level of deputy superintendent of police, to investigate cyber-crimes.

Various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891 and Reserve Bank of India Act, 1934 have been suitably amended to meet the new requirements of e-commerce and cyber-crime investigation.

The IT (Amendment) Act 2008, also referred to as ITAA 2008 introduced major amendments in the IT Act, 2000 primarily pertaining to cyber-crime. It was passed by Lok Sabha on December 22, 2008 and by Rajya Sabha on December 23, 2008.

The ITAA 2008 introduced additional definitions of cyber café, cyber security, electronic signatures, electronic signature certificate and intermediary. It also laid down the procedure for authenticating electronic records and delivery of services by service providers. Changes have also been made in the composition and functioning of the Cyber Appellate Tribunal.

However, major changes have been made in Chapter XI (Offences) in the ITAA 2008. Section 66 pertaining to computer related offences has been subdivided into six subsections. Subsections dealing with punishment for sending offensive messages through communication services, punishment for receiving a stolen computer resource or communication device, punishment for identity theft, punishment for cheating by personation by using computer resource, punishment for violation of privacy and punishment for cyber terrorism have been introduced.

Section 67 dealing with punishment for publishing or transmitting obscene material in electronic form has been further sub divided into three subsections. These are: 67A (Punishment for publishing or transmitting of material containing sexually explicit acts, etc. in electronic form).

67B (Punishment for publishing or transmitting of material depicting children in sexually explicit acts, etc. in electronic form); and 67C (Preservation and retention of information by intermediaries).

Section 69A gives powers to the central government to issue directions for blocking public access to any information through any computer resource while Section 69B empowers the central government to monitor and collect traffic data or information through any computer resource for purposes of cyber security. In addition, Section 70B designates the Indian Computer Emergency Response Team as the national agency for cyber incident response.

Section 78 empowers police officer not below the rank of Inspector to investigate any offence under ITAA 2008, while the IT Act 2000 had given similar powers to police officers of the rank of deputy superintendent of police and above.

Singapore Protection from Online Falsehood and Manipulation Act (POFMA) 2019:[87] On May 8, 2019, Singapore passed the POFMA 2019 also known as the Fake News Act. The Act consists of nine parts and 62 sections. There are four main reasons for which the Act has been enacted. First, to prevent communication of false information and institute measures for counteracting the effects of such communication. Second, to prevent the financing, promotion and support of online locations that repeatedly communicate such false content in Singapore. Third, to enable measures to be taken to detect, control and safeguard against coordinated inauthentic behaviour and other misuse of online accounts and bots and lastly, to ensure disclosure of information concerning paid content directed towards a political end.

One of the challenges facing the world community is that who will determine whether the information or news being disseminated in cyberspace is hateful or fake and when, is such news an innocent prank or a law and order problem or a threat to national security. POFMA attempts to resolve this dilemma. As per Article 7, Part 2 of the Act, a news is deemed to be fake and worthy of action if, and only if, it meets two criteria. First, it should be a false statement of fact and secondly, its communication is likely to affect the security of Singapore or it will be prejudicial to public health, safety, tranquillity or finances or, to Singapore's relations with other countries, or influence the outcome of an election; or incite feelings of hatred, enmity/ill will; or diminish public confidence in the state or its institutions. Article 10 of Part 3 of the Act, authorises any minister in the Singapore government to classify news as fake and take appropriate action to deal with such news.

Article 11 of Part 3 concerns "Correction Direction". A Correction Direction can be issued to a person to communicate a Correction Notice (statement nullifying false information and inserting a corresponding true statement and/or its link next to the false statement) within a specified time limit to all persons who have received the false information, and/or publish the correction notice in a newspaper or other print publications of Singapore. Article 12 of Part 3 also empowers the Competent Authority to issue a "Stop Communication" direction. Article 16 of Part 3 also empowers the minister to direct the Information Communication Media Development Authority (IMDA) to order the internet access service provider to disable access to an online location, for all end users by issuing an "Access Blocking Order".

An Internet Intermediary has been classified as a person providing internet intermediary services (like social networking services, search engines, content aggregators, internet based messaging services, video sharing services, etc.). Part 4 of the Act deals with directions to internet intermediaries and providers of mass media services. Article 21 talks of "Targeted Correction Direction" wherein the internet intermediary that has been used as a medium to propagate the false information is required to send a correction notice within a specified time limit to all the end users in Singapore, who had accessed the subject false information. In addition, Article 22 deals with issuance of "*Disabling Directions*" by the internet intermediary to stop access to the end user in Singapore to a specified false information, while Article 28 deals with "*Access Blocking Order*".

Part 5 of the act deals with "Declaration of online locations" (A "declaration" takes place when an online location is responsible for propagating three or more different false statements, subject to active Part 3 and/or Part 4 directions)". Once an online location has been "declared", its owner is thereafter required to inform all end users that access that online location of it. Suitable directions can also be issued to the IMDA to block access to the "declared" online location for a specified period of time.

Part 6 of the Act deals with directions to the internet intermediary to counteract inauthentic online accounts and coordinated inauthentic behaviour. Part 7 of the Act deals with certain other measures while Part 8 specifies appointment of alternate authority, during election periods and other specified periods. The final Part 9 of the act deals with miscellaneous issues.

Major Global Conventions and Agreements

Budapest Convention:[88] The Convention on Cyber-crime or the Budapest Convention was the first international treaty for addressing cyber-crime by addressing key issues of cyber laws, cyber-crime investigation and international cooperation. The convention was adopted by the Committee of Ministers of the Council of Europe on November 8, 2001 and entered into force on July 1, 2004.

As of September 2019, 64 nations have ratified the convention while four nations have signed the convention but not ratified it. Major countries that have not signed the convention include India, China, Russia and Brazil.

The Wassenaar Arrangement: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies[89] is a Multilateral Export Control Regime (MECR) of 42 nations, established on July 12, 1996 in Wassenaar, in the Netherlands. It is the fall out of the previous Cold War era Coordinating Committee for Multilateral Export Control (COCOM). The Wassenaar Arrangement is not a treaty and therefore is not legally binding. India is a signatory to the Wassenaar Arrangement and joined it on December 7, 2017.

The Wassenaar Arrangement was established to provide regional and international security and stability by states exercising greater transparency and responsibility while transferring conventional arms, munitions and dual use goods and technology.

The Wassenaar Arrangement consists of two control lists namely the list of dual use goods and technology (also called basic list) and the munitions list. The list of dual use goods and technology is further sub divided into the sensitive list and the very sensitive list. The basic list comprises of 10 categories including electronics, computers, telecommunications and information security.

Shanghai Cooperation Organisation (SCO):[90] The SCO was established in 2001 and has eight member states namely China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Uzbekistan, India and Pakistan. It is the largest regional organisation in the world in terms of geographical area and population. As part of its Regional Anti Terror Structure (RATS), the SCO has an active cyberspace programme including conduct of cyber anti-terrorism exercises. The SCO has also been proactive in placing an International Code of Conduct on Information Security before the UN General Assembly.[91]

Paris Call:[92] The Paris Call for trust and security in cyberspace was given by French President Emmanuel Macron on November 12, 2018 at the *United Nations Educational, Scientific and Cultural Organisation (UNESCO)* Internet Governance Forum (IGF) and is a high level declaration for developing common principles for securing cyberspace. A total of 67 states including India, 139 international and civil society organisations and 358 private sector entities have supported the Paris Call.

The Paris Call is based on nine principles which are: protect individuals and infrastructure; protect the internet; defend electoral processes; defend intellectual property (IP); non-proliferation; lifecycle security; cyber hygiene; no private hack back; and international norms.

Conclusion

Cyberspace is presently in the midst of tremendous change and upheaval, the likes of which have not been witnessed before. Technological barriers are being broken at break neck speed with newer and newer technologies are surfacing even before the latest ones have matured and stabilised. More than half of the world's population is using internet and the number of mobile phones and computing devices have surpassed the global population. Advances in backbone network technologies like Dense Wave Division Multiplexing have ensured availability of almost limitless bandwidth at very little cost, which coupled with mass supply of high end cheap processors and unlimited cloud storage has broken down the entry barriers and flattened the curve in favour of cognition over capital.

Disruptions in the cyberspace arena have picked up speed like never before. So much is happening so fast, that it is nearly impossible to keep pace with the advancements and predict the future. Disruptive technologies like AI, Block chain, IoT, Big Data Analysis, robotics, 3D printing, and autonomous vehicles have almost reached a tipping point and are set to change the way the world connects, transacts, socialises and fights war. Newer technologies like Quantum and Nano technologies are also being tested and are round the corner.

AI is the ability of the machine to perform cognitive tasks like thinking, perceiving, learning, problem solving and decision, making akin to humans. This has given way to a number of AI related fields like facial recognition, image processing, audio processing, natural language processing and machine learning. In addition, a large number of AI driven predictive and decision making algorithms are being used across the length and breadth of various industries ranging from medical diagnostics to weather forecasting.

There are broadly three pre requisites for developing an accurate AI system. First is the availability of large quantity of data for a given data set so that the AI system can be first trained and thereafter use the data set to further train and improve itself. Second, a suitable AI algorithm which can accurately match the user requirement to a desired output and lastly fast processing ability so that enormous quantity of data can be churned quickly and repeatedly to quantitatively improve the AI system performance. There has been exponential improvement in all the above three pre-requisites over the last decade or so which has resulted in AI systems that are highly sophisticated and way better at performing some real life jobs than humans.

Robotics coupled with AI will greatly impact employment and the workforce across the globe. Autonomous vehicle technology will drastically impact the transportation industry where the demand for professional drivers will reduce sharply. The manufacturing industry has already witnessed drastic job cuts due to large scale automation of processes. Even the legal, financial sector, insurance, bureaucracy and back office operations will be greatly impacted. Some also argue that AI will usher in an era of creativity, well-being and prosperity as people will be free from performing monotonous fixed time jobs and will move towards a more flexible and rewarding work-life balance.

AI will also transform warfighting. From war gaming and scenario prediction to real time contingency planning and decision making, most of the complex cognitive processes associated with intelligence, prediction, analysis and decision making during conflict will be performed by AI based smart integrated systems. Smart munition and autonomous vehicles and delivery systems will greatly increase the lethality and accuracy of strikes resulting in fast paced and violent conflicts.

Block chain based digital currency is being used the world over as financial instruments especially for illicit activities and converting corruption money. Block chain technology which is based on digital, decentralised and distributed ledger system can transform the way records and transactions are verified and stored on the web. It can track and monitor the movement of sensitive items and raw materials around the world and has a host of other uses ranging from digital IDs to smart contracts and payments.

IoT will usher in an era of *smart* wearables and household equipment like watches, clothes, lights, fridges, doors and air conditioners. The humongous amount of data generated by IoT devices will further optimise and refine the AI systems of the future. Coupled with it is the fear of growing cyber-crime and cyber espionage, as cheap smart wearables and devices are likely to be more vulnerable to hacking and manipulation.

Recently, there are growing concerns relating to user digital privacy concerns. The Snowden revelations of 2013 highlighted the way social media and other multinational IT companies were keeping tabs on individual user private data and sharing it with various intelligence agencies across the world. There have also been instances of the mass sale of user public data to third parties. In the famous Cambridge Analytica data breach scandal, the whistle-blower Christopher Wylie had revealed the sheer scale of the harvesting of millions of Facebook profiles to predict and influence choices during elections. He also revealed that Facebook had since 2015, been aware that user's privacy data was being harvested on an unprecedented scale and yet had hardly taken any measures to secure the confidential data.

With the enormous advances being made in the field of AI and Big Data Analysis, data has become a very important and precious commodity. It is therefore no surprise that massive hacking attacks to steal the users' private data have taken place over the last five years. Topping this list are the three billion Yahoo accounts in 2013-14 followed by Marriott International (500 million between 2014-18), Adult Friend Finder (412.2 million in October 2016), eBay (145 million in May 2014) and Equifax (143 million in July 2017).[93]

Weaponisation of cyberspace is a harsh reality which each one of us has to face. Lack of international laws coupled with a large reach, low cost, anonymity, lack of attributability and ease of delivery make the cyberspace an ideal medium for cyber-attacks and psychological warfare, by both state and non- state actors.

The Centre for Strategic and International Studies (CSIS), Washington, D.C. has published a list of significant cyber incidents and activities carried out since 2006.[94] The list gives out in detail the various cyber war related activities carried out by different state and non-state actors. These include: Stealing of intellectual property and trade secrets; stealing of private data; psychological campaigns to influence elections; monitoring of communication channels; interfering in critical infrastructure systems like electricity and banking, etc.; and causing serious malfunction in critical components linked to oil production and nuclear energy. The sheer scope and magnitude of cyber warfare related activities being carried out continuously around the globe is mind boggling and scary.

The spurt in cyber-crime and cyber espionage and warfare related activities has prompted a number of countries to take stringent measures like data localisation and meta data tracking and analysis, resulting in fragmentation of the internet. Cyber sovereignty as a term has caught the fancy of many nations, who favour having their own customised and sanitised internet.

The bulk of cyberspace is being run and managed by a handful of mega ICT companies who have almost assumed the size, economy and stature of nation states. These companies have business interests across the length and breadth of the globe and walk a tight rope while dealing with the national security concerns of various countries, especially when dealing with two or more states having adversarial relations with each other. The mega ICT companies are slowly beginning to realise that they not only deal with business interests, but are also intimately linked with the national security of the countries in which they are operating.

An attempt has been made to present a brief overview of the cyberspace domain as it is felt that sometimes its sheer complexity leads to a myopic view point, especially when dealing with strategic issues which need understanding of a higher plane, or what is sometimes referred to as “helicopter vision”. A lot can be said and written about the cyber domain but one thing is certain: It is the domain of the future and mastery over it is essential as it not only provides extraordinary benefits and leverage but is also crucial for a nation state’s well-being and survival, just like the natural domains of land, sea and air.

Notes

1. Moore, Gordon E, “Cramming more components onto integrated circuits”, *Electronics*, April 19, 1965 at https://drive.google.com/file/d/0By83v5TWkGjvQkpBcXJKT1I1TTA/view, accessed on July 31, 2018.
2. https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/, accessed on July 27, 2018.

3. https://www.itu.int/net/ITU-R/index.asp?redirect=true&category=information&rlink=terminology-database&lang=en#lang=en, accessed on August 1, 2018.
4. NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD-54 HOMELAND SECURITY PRESIDENTIAL DIRECTfVEIHSPD-23, p. 3 at http://www.lloydthomas.org/5-SpecialStudies/nspd-54Jan08.pdf accessed on August 2, 2018.
5. https://blogs.cisco.com/security/cyberspace-what-is-it, accessed on August 2, 2018.
6. Foreword by DG IDSA, Cherian Samuel and Munish Sharma, *Securing Cyberspace: International and Asian Perspectives*, Pentagon Press, New Delhi, 2016.
7. Daniel T. Kuehl, 'From Cyberspace to Cyberpower : Defining the Problem', in *Cyber Power and National Security,*Vij Books, New Delhi, June 2009, p. 28.
8. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, accessed on August 6, 2018.
9. https://www.statista.com/statistics/204954/average-internet-connection-speed-worldwide/, accessed on August 6, 2018.
10. http://www.sciencefocus.com/qa/how-many-terabytes-data-are-internet, accessed on August 7, 2018.
11. International Telecommunication Union 2017 report on percentage of individuals using the internet at https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx, accessed on August 7, 2018.
12. https://www.backblaze.com/blog/hard-drive-cost-per-gigabyte/, accessed on August 10, 2018.
13. https://www.genome.gov/images/content/costpermb_2017.jpg, accessed on August 10, 2018.
14. https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf, accessed on August 16, 2018.
15. Greg Austin, "Middle Powers and Cyber-Enabled War: The imperative of collective security", in Cherian Samuel, Munish Sharma eds. *Securing Cyberspace*, Pentagon Press, New Delhi, 2016, p. 38.
16. For additional details on GGE and OEWG go to https://dig.watch/processes/un-gge#view-7541-4, accessed on January 27, 2020.
17. https://www.cambridge.org/in/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB, accessed on August 20, 2018.
18. Adam Firestone, 'In Cyberspace, Anonymity and Privacy are Not the Same' at https://www.securityweek.com/cyberspace-anonymity-and-privacy-are-not-same, accessed on August 21, 2018.

19. The Department of Defence Cyber Strategy, April 2015 at http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf, accessed on September 6, 2018.
20. https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/, accessed on September 6, 2018.
21. https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/, accessed on September 6, 2018.
22. https://www.statista.com/statistics/735904/worldwide-x86-intel-amd-market-share/, accessed on September 17, 2018.
23. https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/, accessed on September 17, 2018.
24. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150, accessed on September 17, 2018.
25. http://www.tech-faq.com/history-of-computer-viruses.html, accessed on September 17, 2018.
26. https://en.wikipedia.org/wiki/Harry_Nyquist, accessed on October 24, 2018.
27. Report of the Working Group on Internet Governance, Chateau de Bossey, June 2005, at https://www.wgig.org/docs/WGIGREPORT.pdf, accessed on November 22, 2018.
28. Peter J. Katzenstein, ed., *The Culture of National Security: Norms and Identity in World Politics,* Columbia University Press, New York, 1996, p. 5.
29. Martha Finnemore, "*Cybersecurity and the concept of norms*", Carnegie Endowment for International Peace at https://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870, accessed on November 27, 2018.
30. Joseph S. Nye, Jr, *"The Regime Complex for Management Global Cyber Activities",* Global Commission of Internet Governance (GCIG) and Chatham House, Paper series: No. 1 – May 2014.
31. Ibid.
32. https://www.itu.int/en/about/Pages/whatwedo.aspx, accessed on December 11, 2018.
33. https://www.ietf.org/, accessed on December 13, 2018.
34. https://www.icann.org/, accessed on December 13, 2018.
35. https://www.icann.org/news/announcement-2013-10-07-en, accessed on December 13, 2018.
36. https://www.w3.org/, accessed on December 13, 2018.
37. https://www.first.org/, accessed on December 14, 2018.

38. https://www.ieee.org/, accessed on December 14, 2018.
39. Courtesy *Cyber Crime – A to Z Glossary of Terms* at https://www.newsletter.co.uk/news/crime/cyber-crime-a-to-z-glossary-of-terms-1-8068408, accessed on November 15, 2018 and *Glossary of Cybercrime Terms* at https://dealers-insurance.com/glossaryofcybercrimeterms.php, accessed on November 15, 2018.
40. For more information see UNESCO's "Journalism, 'Fake News' and Disinformation Handbook for Journalism Education and training" at https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0_0.pdf, accessed on February 1, 2020.
41. For more details, go to https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, accessed on February 2, 2020.
42. For full judgement go to https://www.echr.coe.int/sites/search_eng/pages/search.aspx, accessed on August 8, 2019.
43. For more on the judgement go to https://www.washingtonpost.com/opinions/the-supreme-court-just-struck-a-blow-against-mass-surveillance/2018/06/25/1b5ee510-7653-11e8-b4b7-308400242c2e_story.html?noredirect=on&utm_term=.792597710f63, accessed on February 3, 2020.
44. For more details read World Economic Forum's White paper 'Internet fragmentation: An Overview' at http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, accessed on February 3, 2020.
45. For more information on the subject go to https://www.bbc.com/news/technology-50902496, accessed on February 4, 2020.
46. For more information go to https://www.csoonline.com/articl e/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html, accessed on February 4, 2020.
47. Nick Ismail, "Global Cybercrime economy generates over 1.5 Tn, according to new study", *Information Age,* April 24, 2018 from https://www.information-age.com/global-cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/, accessed on February 4, 2020.
48. *Symantec Internet Security Threat Report Volume 24*, February 2019 at https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf, accessed on November 18, 2019.
49. Steve Morgan, "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics", Cisco and Cybersecurity Ventures Press Release, February 6, 2019 at https://cybersecurityventures.com/cybersecurity-almanac-2019/, accessed on November 14, 2019.
50. Megan Burns, "Information Warfare: What and How" at https://www.cs.cmu.edu/~burnsm/InfoWarfare.html, accessed on December 19, 2018.
51. Martin C. Libicki, " What is Information Warfare?" at http://www.dodccrp.org/files/Libicki_What_Is.pdf, accessed on December 20, 2018.

52. US Joint Publication 3-13, "Information Operations" at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, accessed on December 20, 2018.
53. US Joint Publication 3-12, "Cyberspace Operations" at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150, accessed on December 20, 2018.
54. David S. Alberts, John J Garstoka, Fredrick P Stein, "*Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd edition (Revised)*", DOD CSISR Cooperative Research Programme, p. 2 at http://www.dodccrp.org/files/Alberts_NCW.pdf, accessed on December 20, 2018.
55. Note 40.
56. Note 43.
57. Summary of the 2018 "National Defence Strategy of the United States of America-Sharpening the American Military's Competitive Edge" at https://admin.govexec.com/media/20180118173223431.pdf, accessed on December 27, 2018.
58. Summary of the Department of Defence Cyber Strategy 2018 at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF, accessed on December 28, 2018.
59. Michael S Schmidt and David E Sanger, "5 in China Army Face US Charges of Cyber Attack", *New York Times,* May 20, 2014, digital edition at https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html, accessed on December 28, 2018.
60. Press Release of US Department of Justice at https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations, accessed on December 28, 2018.
61. FBI press release at https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018, accessed on December 28, 2018.
62. For detailed story go to https://www.natlawreview.com/article/doj-announces-more-equifax-charges-credits-chinese-hackers, accessed on February 15, 2020.
63. Note 25.
64. Ministry of National Defence, The People's Republic of China, "Strategic Guideline of Active Defence" at http://eng.mod.gov.cn/Database/WhitePapers/2015-05/26/content_4586711.htm, accessed on December 31, 2018.
65. Cortez A Cooper, "PLA Military Modernization: Drivers, Force Restructuring and Implications", Testimony before the US China Economic and Security Review Commission of February 15, 2018 at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT488/RAND_CT488.pdf, accessed on December 31, 2018.

66. Deepak Sharma, "Integrated Network Electronic Warfare: China's New concept of Information Warfare", *Journal of Defence Studies,* IDSA at https://idsa.in/system/files/jds_4_2_dsharma.pdf, accessed on December 31, 2018.
67. White Paper on "China's Military Strategy" at http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm, accessed on December 31, 2018.
68. China's National Cyberspace Security Strategy at http://www.cac.gov.cn/2016-12/27/c_1120195926.htm, accessed on July 17, 2018.
69. *Russia National Security Strategy to 2020* at http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020, accessed on January 2, 2019.
70. "*The Military Doctrine of the Russian Federation*" at https://rusemb.org.uk/press/2029, accessed on January 2, 2019.
71. *Russian National Security Strategy* at http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf, accessed on January 2, 2019.
72. *Doctrine of Information Security of the Russian Federation* at http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, accessed on January 3, 2019.
73. Timothy Thomas, 'Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?', *The Journal of Slavic Military Studies*, 27:1, 101-130, DOI: 10.1080/13518046.2014.874845 at https://www.tandfonline.com/doi/pdf/10.1080/13518046.2014.874845, accessed on January 3, 2019.
74. Kara Flook, 'Russia and the Cyber Threat', May 13, 2009 at http://www.criticalthreats.org/russia/ russia-and-cyber-threat, accessed on January 13, 2019.
75. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare", *CAN Occasional Paper Series,* March 2017 at https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf, accessed on January 3, 2019.
76. Telecom Regulatory Authority of India (TRAI) press release No 50/2017 dated July 13, 2017, "*Highlights of Telecom Subscription Data as on 31st May 2017*" at https://trai.gov.in/sites/default/files/Press_Release_No50_Eng_13072017.pdf, accessed on January 4, 2019.
77. *Financial Express* (24 May 2017). "'India's digital economy set to grow from $270 bn to $1 tn by 2024', says Ravi Shankar Prasad" at http://www.financialexpress.com/economy/indias-digital-economy-set-to-grow-from-270-bn-to-1-tn-by-2024-says-ravi-shankar-prasad, accessed on January 4, 2019.
78. Rajya Sabha TV online edition, "Cyber crime rose between 2014 and 2017, Govt tells Parliament" January 5, 2018 at https://rstv.nic.in/cyber-crimes-rose-2014-2017-govt-tells-parliament.html, accessed on January 4, 2019.

79. International Telecommunication Union (ITU), *Global Cyber Security Index* at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, accessed on January 4, 2019.
80. Ministry of Electronics and Information Technology (MeitY), *National Cyber Security Policy 2013* at http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf, accessed on January 4, 2019.
81. Headquarters Integrated Defence Staff, Ministry of Defence, "Joint Doctrine Indian Armed Forces" at https://bharatshakti.in/wp-content/uploads/2015/09/Joint_Doctrine_Indian_Armed_Forces.pdf, accessed on January 9, 2019.
82. "European Union General Data Protection Regulations" at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed on January 10, 2019.
83. A *controller* is the entity that determines the purposes, conditions and means of the processing of personal data, while the *processor* is an entity which processes personal data on behalf of the controller.
84. The US *Federal Information Security Management Act* at https://www.govinfo.gov/content/pkg/STATUTE-116/pdf/STATUTE-116-Pg2899.pdf, accessed on January 10, 2019.
85. English translation obtained from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/, accessed on January 14, 2019.
86. The Information Technology Act – 2000 at http://dot.gov.in/sites/default/files/itbill2000_0.pdf, accessed on January 16, 2019.
87. For complete document go to https://www.parliament.gov.sg/docs/default-source/default-document-library/protection-from-online-falsehoods-and-manipulation-bill10-2019.pdf, accessed on February 3, 2020.
88. For more details on the Budapest convention go to https://www.coe.int/en/web/cybercrime/the-budapest-convention, accessed on February 5, 2020.
89. The founding document can be accessed at https://www.wassenaar.org/app/uploads/2019/consolidated/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf, accessed on February 6, 2020.
90. For more information go to http://eng.sectsco.org/, accessed on February 5, 2020.
91. Cherian Samuel and Munish Sharma, *Ïndia's Strategic Options in a Changing Cyberspace*, IDSA, Pentagon Press, New Delhi, 2019, p. 66.
92. For more details go to https://pariscall.international/en/, accessed on February 6, 2020.

93. Taylor Armerding, “The 18 biggest data breaches of the 21st century” at https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html, accessed on January 18, 2019.
94. Centre for Strategic and International Studies (CSIS),”Significant Cyber Incidents” at https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity, accessed on January 18, 2019.

3. Artificial Intelligence as a Strategic Force Multiplier

It is not my aim to surprise or shock you – but the simplest way I can summarize is to say that there are now in the world machines that think, that learn and that create. Moreover, their ability to do these things is going to increase rapidly until – in a visible future – the range of problems they can handle will be coextensive with the range to which the human mind has been applied.

– Herbert Simon (1957)

AI will be either the best, or the worst thing, ever to happen to humanity.

– Stephen Hawking (1942-2018)

Introduction

Artificial Intelligence or AI has taken the world by storm. People from all walks of life, be it students, academicians, scientists, policymakers, businessmen, soldiers, farmers, doctors, car drivers, house wives, showmen, journalist get excited whenever the term AI is mentioned. It might be an altogether different matter that each one's definition, perception or knowledge of what AI really is and what it can achieve might be in complete disagreement with one another, or at times be diametrically opposite.

Niti Aayog in its discussion paper titled "National Strategy for Artificial Intelligence #AIFORALL"[1] has acknowledged that, "AI might just be the single largest technology revolution of our live times, with the potential to disrupt almost all aspects of human existence." The global investments in AI are expected to reach $89.85 billion in 2025 from approximately $3.2 billion in 2016.[2] The west, especially the US has taken the global lead in this niche yet highly disruptive technology. The major AI players are Amazon, IBM, Siemens, Google AI, Omron Adept Technologies, AI Brain, Apple, Facebook, Microsoft and Anki.[3]

The concept of AI is not new and has been on and off discussed since the early 1950s. Issac Asimov wrote many stories about robots and his first collection *I, Robot* talked of "robopsychology" which delved into the study of robot minds and psychology and what happened in their "positronic brains". He laid down the three laws for robots that ensured they would cause no harm to humans or humanity either through action or inaction.

In 1950s Alan Turing proposed the "Turing Test" to validate the capabilities of a machine to think and act as a human. According to the test if a human interrogator poses certain questions and after analysing the answers is unable to distinguish that the answers came from a human or a machine then, it would have passed the benchmark of being labelled as "Artificially Intelligent". To pass the Turing test the machine would need to be an expert in the following disciplines. First, "Natural Language Processing" in order to process the spoken questions of the human interrogator and then to convert them into set of machine capable problems. Second, "Knowledge Representation" to store and retrieve relevant information from a digital repository. Third, "Automated Reasoning" to draw logical conclusions and provide relevant answers from its stored repository of information for the questions posed by the human interrogator and lastly, "Machine Learning" to adapt to newer types of questions by learning from past questions and answers, in essence self-learning and improvement on the basis of past experiences and feedback. In order to pass the Turing Test, the machine would also require "Computer Vision" or sensory capabilities to perceive objects and "Robotics" in order to act as per instructions given by the intelligent machine. Thus, the Turing Test not only defines the different subsets of what we broadly constitute as AI, but it also establishes its relevance to this day.

In 1956, John McCarthy, who is regarded as the father of AI conducted a two month, 10 man study on AI (a term coined by him), at Dartmouth College, Hanover, New Hampshire. The study encompassed a wide range of topics like, complexity theorems, language simulation, neuron nets, content abstraction from sensory inputs, relationship of randomness to creative thinking and learning machines. The Dartmouth Conference put forth a vision of the enormous capabilities of AI, which generated tremendous interest, research and development in this new and exciting field of intelligent machines.

In the early 1970s, the British Science Research Council asked Sir Michael James Lighthill (1924-1988), a world renowned mathematician to review the academic research into AI. Lighthill in his report[4] divided AI into three categories: Category A (Advanced automation); Category C (computer based Central Nervous System (CNS) research); and Category B (bridge between category A and C or building Robots category). He said in his report that very limited success had been achieved in Category A and Category C while work in Category B has been largely disappointing. Disappointments in Category A were in pattern and speech recognition, machine translation, natural language processing and mathematical theorem proving that there had been some successes in the heuristic dendral programme for inference of chemical structure from mass spectroscope data. Most of the work in Category C dealing with neural networks fell in the disappointing category with success in the field of psychology especially psycho-linguistics. The report was the reason for the British government to stop funding AI research in all universities except Edinburgh, Sussex and Essex and led to the first AI winter which continued from 1974 to 1980.

Another impediment to the growth of AI in 1970s was the problem of "combinatorial explosion" wherein the computation time required to solve certain types of problems increased exponentially with the increase in variable size of the problem. Common example of combinatorial explosion are games like Sudoko and Chess. Nondeterministic Polynomial time (NP) hard problems are a subset of combinatorial explosion problems wherein there are no algorithms existing which can accurately solve the given problem. Most of the problems that AI endeavoured to solve fell into the domain of NP hardness.

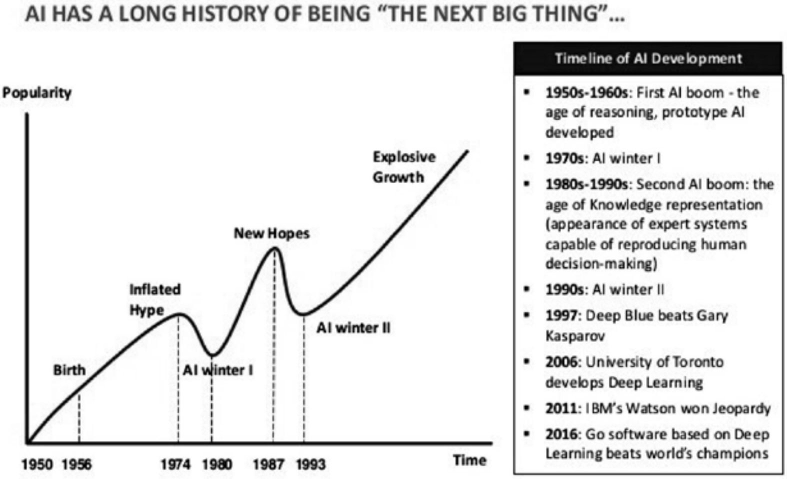
Between 1980 to 1987, interest in AI picked up momentum. AI specific hardware and software like LISP[5] (the second oldest programming language after FORTRAN. Preferred by AI enthusiasts due to its strong mathematical base and use of linked lists), XCON (short for expert configuration is used to automatically select DEC's VAX computer system components based on user requirements) and symbolic (computer hardware designed to run the Lisp software) became popular and AI based decision making programmes to target specific niche problems identifying certain chemical compounds or medical diagnosis of specific diseases (like MYCIN programme) gathered momentum.

From 1987 to 1993, enthusiasm for AI again waned giving rise to AI winter II primarily due to the large scale availability of desktop computers from IBM and Apple, which did away with the need of specific high end computers for running LISP and other AI specific programmes.

Interest in AI picked up when ISX corporation won the US government's Defence Advanced Research Projects Agency (DARPA) contractor for the year award in 1993 for the AI based Dynamic Analysis and Replanning Tool (DART) programme which was extensively used by the US military to fulfil a number of its logistic problems notably the optimisation of the movement of supplies and personnel. It is reported that the savings brought about by DART programme more than made up the DARPA's investments in the field of AI since the 1950s.

In 1994, two autonomously driven cars VaMP and VITA-2 (standard grey Mercedes SEL cars fitted with autonomous driving systems) designed and fabricated by German aerospace scientist Ernst Dickmanns in collaboration with Daimler-Benz carried passengers and drove more than a thousand kilometres on a busy Paris three lane highway with maximum speed of up to 130 kmph.[6] The race for driver less vehicles had begun.

Another major milestone was achieved in 1997, when 'Deep Blue', an AI based chess programme of IBM defeated world chess champion Gary Kasparov.[7] A total of two matches of six games each were played between the two. The first match was played in Philadelphia in 1996 which was won by Gary Kasparov 4-2. The rematch was held in New York City in 1997 and was won by Deep Blue $3\frac{1}{2}-2\frac{1}{2}$. In March 2016, 'AlfaGo', the AI based computer programme of Google's Deep Mind defeated Lee Seedol a 9 dan professional and reigning Go champion by 4-1. The Go is the most complex board game of 9x9 squares designed by man.



- **1950s-1960s**: First AI boom - the age of reasoning, prototype AI developed
- **1970s**: AI winter I
- **1980s-1990s**: Second AI boom: the age of Knowledge representation (appearance of expert systems capable of reproducing human decision-making)
- **1990s**: AI winter II
- **1997**: Deep Blue beats Gary Kasparov
- **2006**: University of Toronto develops Deep Learning
- **2011**: IBM's Watson won Jeopardy
- **2016**: Go software based on Deep Learning beats world's champions

Source: Actuaries Digital

Presently AI covers a wide range of industries, technologies and processes. From the ubiquitous Siri and Alexa voice activated assistants to advanced face and voice recognition systems, autonomous vehicles, bio-medicine, numerous decision making and optimisation systems, weather forecasters, gaming devices and software, robotics, taxi aggregators … the list is endless. In fact there can be hardly any area of human endeavour which is out of the reach of AI.

It is quite obvious that AI will make enormous inroads into the business of warfighting owing to its widespread employability over a host of different and sometimes uncorrelated fields as well as the overall force multiplication effect produced by it. Also, bulk of the initial funding for the AI research and development, especially in the US was provided by its Department of Defence (DoD).

One question which almost everyone asks is how is AI different from earlier computer programmes. In a non AI computer programme, there is an input which is fed into the computer and an output is derived after the algorithm analyses the input and processes it as per a given set of instructions. The entire sequence of actions starting from taking the input, processing it and producing the output is known and written by the programmer. For the same input, we will always get the same output irrespective of the number of times the computer programme is run.

In AI, things are slightly different. For starters, it is not necessary that for the same input you will get the same output, every time. AI tries to solve problems which are NP hard and therefore rather than finding exact solution, AI endeavours to use large quantities of data and probability to find good solutions. Second, the programmer cannot predict the way the machine has actually processed the input to arrive at the output. The processing of input by the computer is largely unknown. If you know the exact steps taken by the computer to process the input to arrive at output, then it is no longer AI. Third, AI programmes are self-improving. The quality of result keeps on improving as more and more data is fed and iterations are carried out by the AI programme.

Most AI programmes are developed in three stages namely learning, testing and fielding. In the learning stage, the AI programme is provided a large data set of annotated data and it tries to self-learn from this learning data by using an iterative process of continuous self-improvement. It is therefore extremely important that the learning data set provided to the AI programme is clean, very well annotated and without any bias. In the testing stage, fresh test data is fed to the AI programme to judge the quality of output produced by the programme. After thorough learning and testing stages, the AI programme is finally fielded and allowed to interact with live data to produce results.

A detailed tutorial on essentials of AI that includes the AI model, types of environments and agents, search and adversarial problems, knowledge representation, working under uncertainty, decision making by intelligent agents and learning systems is given at Appendix B.

Major Sub-Areas of AI

Natural Language Processing (NLP): The World Wide Web has over one trillion web pages which are filled with information. NLP assumes significance as it is essential for text classification, information retrieval and information extraction from the web. A programming language has a fixed syntax of representation which makes it very easy to interpret and work in the digital domain. Natural languages on the other hand, in spite of having a grammar, make a number of mistakes in sentence formation and convey ambiguous information. Also, natural languages are extremely extensive and constantly changing. Thus, deciphering, categorising and extracting information from natural languages by the intelligent agent is a difficult task. The agent tackles this problem by breaking down natural languages into probability distribution of different sets of sentences. N-gram character models are generally used with n representing the number of letters in a sentence. Some of the tasks given to the intelligent agent are language identification (whether language is English, German or Spanish, etc.), spelling correction, genre classification (whether it is a legal document, medical prescription, scientific article, spam mail, etc.) and named-entity (finding names in a document and deciding the class to which they belong as for example the name of a drug in a medical prescription) recognition.

A basic information retrieval system consists of four things. First, a collection of documents. Second, query/queries from the user. Third, result set based on query/queries posed and lastly, presentation of the result set. Most information retrieval systems have a scoring system based on which the result set is presented to the user (Usually in descending order. For example from the latest web page having most relevance to search key words down till the oldest page with least relevance). A page rank algorithm and Hyper

Link-Induced Topic Search (HITS) algorithm are commonly used information retrieval algorithms.

Automaton Parsing is the method used for analysing a sequence of words to uncover their structure according to grammar. Probabilistic Context Free Grammar (PCFG) is a method of automating sentence formation based on a set of rules derived from natural languages. It involves assigning probabilistic weightages to sentences in order to arrive at the most appropriate sentence for a given meaning. PCFGs have also been successfully used for the probabilistic modelling of Ribonucleic Acid (RNA) structures.

Machine translation is the process of automatically translating text from one language to another. Machine translation is considered difficult as words in one language may have multiple meanings and thus multiple words in a different language. Interlingua is a type of intermediate language that represents all the different variations between two different languages. Machine language translation can be done by three methods. The first method is by Interlingua knowledge representation. It is considered difficult as firstly one needs to have the complete knowledge representation of a given sentence, thereafter automatically parsing it and finally generating the sentence into the translated language. The second method is by transfer mode. Here a database of translation rules (multiple examples) are maintained between the set of languages and as and when, a match occurs in one language, its corresponding sentence is given as an output in the translated language. The third method is by Statistical Machine Translation. This involves training a probabilistic based intelligent machine on a huge library of data accumulated for the set of different languages.

Speech Recognition: A large number of present day applications like "Siri" of Apple and "Alexa" of Amazon rely on AI based speech recognition systems. Human speech varies in frequency from 100 Hz to 1000 Hz and a standard Analog to Digital (A to D) convertor requires roughly 500 kilo bytes of data to store a minute of speech.

There are about 100 speech sounds called "phones" which can be used to pronounce all the words in all the known languages. The smallest unit of sound that has a particular meaning in a given language is called “phoneme”. To recognise speech, first it is broken down into time slices or frames with each frame roughly of 10 milliseconds duration. Thereafter, the samples in each frame are subjected to Fourier transform to determine the acoustic amplitude at ten to twelve frequencies. Thereafter the Mel Frequency Cepstral Coefficient (MFCC) is computed for each of the frequencies in the frame and the overall acoustic energy of the frame. Thus, each frame now has 13 attributes (MFCC of 12 frequencies and one overall frame acoustic energy).

Using each frame as a percept, the Hidden Markov Model (HMM) algorithm is used to find the variations in the precept sequence to arrive at the various phones used during multiple frames which when mapped with the word set of a particular language, give rise to the understanding of words spoken and subsequently the combination of words into sentences takes place based on N-gram model of NLP. As the learning based intelligent agent is subjected to audio inputs over a period of time, it is able to improve its recognition of words and framing of sentences and can also be used to distinguish between voices of different people or recognising specific emotions expressed during speaking various sentences.

Computer Vision/Image Recognition: Making sense and extracting knowledge from visual images is one of the major areas of research of AI. It assumes importance because of the unprecedented numbers and types of image recording devices available in the world and the sheer quantity and quality of high impact applications, which can be developed. Some of the major applications which use AI based visual intelligent agents are satellite imagery interpretation, autonomous vehicle environment maps, spectral image resolution and imagery interpretation for agriculture, climate change, hydrography, etc. and facial recognition systems.

One of the problems associated with images is the large quantity of data generated and its subsequent analysis and interpretation in real time. A high end robotic eye for microscopic surgery can generate up to 10 GB of data per minute. The problem for the intelligent visual agent is to find out which part of the image is to be analysed and taken into consideration for making a rational decision and which part is to be discarded.

The visual sensory model consists of the object model (it contains the set of all objects available in the environment along with their typical attributes) and the rendering model (it describes the physical, geometric and statistical processes that has produced the image as a sensory percept to the visual intelligent agent).

Edge detection, texture and computation of optical flow are three major ways to convert a raw image/video into an intelligent image/ video that is capable of analysis and processing by the intelligent visual agent in real time. Segmentation is the process of converting an image into various objects (areas of the image having pixels of similar attributes of brightness, colour, texture, etc.) with well-defined boundaries. Edge detection is used to convert the image into well-defined objects based on identifying the edges between various objects which can thereafter be analysed by the intelligent visual agent due to lessor memory size and geometric modelling of image. Edge detection is quite effective for smooth images however, in case of images with texture (visual similarity of various portions of the image. For example the stripes of zebra in an image of zoo), finding the boundary between various objects becomes a problem which is resolved by differentiating objects based on their texture. Optical flow is the relative motion in a series of images when shot as a video. It provides the direction and speed of motion and is also useful for identifying the useful portions of the image which need detailed analysis and the relative distance between objects to resolve the near far problem (nearer objects move faster in comparison to farther objects from the perspective of the camera used to shoot the video).

There are three methods to implement the intelligent visual agent. In the Feature Extraction method the attributes of an object are extracted from the image and mapped to the available object model, in order to identify objects in the image. In the Recognition method interpretation of the image is done by making use of the visual sensory input as well as other inputs available with the intelligent visual agent, to improve accuracy and quality of interpretation. In the Reconstruction method, the agent builds a geometrical model of the environment from the image/set of images given as sensory input to it.

Robotics: Robots are machines that are capable of performing a variety of tasks in the real world. Robots have a sensor/s to perceive the environment and effectors (legs, wheels, tracks, grippers, joints, etc.) for carrying out physical activity in the environment. Robots are largely divided into three categories. The manipulators are physically anchored and are generally equipped with joints and grippers to perform a variety of tasks usually on the factory floors. The next category of mobile robots consists of both the Unmanned Ground Vehicles (UGV) as well as the Unmanned Aerial Vehicles (UAV). The last category are the mobile manipulators, which are a combination of the previous two categories. One of the complexities of robotics is that robots operate in the real world environment which is generally random and partially observable. Also, learning to perform in a real world environment cannot be achieved in isolation, like learning how to play chess by going through thousands of previous game situations, but has to be carried out in real world which is not only time intensive but can also result in physical damage and harm.

Nowadays robots are equipped with a wide variety of sensors ranging from: cameras (optical, infra-red, thermal, stereo vision, etc.); range finders (sonar, LIDAR (Light detection and ranging), etc.); radars; tactile sensors (whiskers, bump panels; touch sensitive skin, etc.); geo locators (GPS); proprioceptive sensors (systems which inform the robot of its own motion); shaft decoders (calculating wheel/shaft rotation for odometry); inertial systems (gyroscopes); force and torque detectors, etc.

Degree of Freedom (DOF) is a term used to specify the way in which a robot can manipulate its effector/s for carrying out various tasks. One DOF refers to an independent direction in which the effector can move. A six DOF refers to three coordinates in space (x, y and z axis) and three angular coordinates (yaw, roll and pitch). Highly precise effectors can have seven or more DOFs for carrying out complex and precision tasks. Another important component in a robot is its power source which can range from an electric motor to hydraulic and pneumatic sources.

An intelligent robot should be able to know its exact location and that of various objects in the environment at all times, process various inputs from sensors, take rapid variations in sensor data into consideration and thereafter make rational decisions based on the above inputs. Thus AI plays a major role in processing the percept sequence and adapting the robot to new stimulus while making rational decisions. The complexity of AI systems of a mobile manipulator like an autonomous drone will be much more than that of a simple manipulator like an industrial robot on the shop floor.

Other AI Issues

Where has AI reached?: There has been a lot of hype created around the capabilities and super human intelligence of AI systems. Recent years have seen the rapid advancement and usage of AI enabled technologies which have improved productivity and efficiency manifold. There have also been a number of setbacks and limitations in the technology, which are not widely discussed.

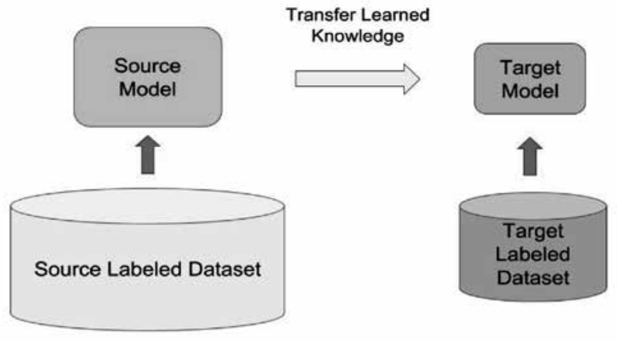
- **Learning Systems:** There has been tremendous improvement in AI based learning systems and this field offers enormous potential for exploitation. The major drivers of Learning systems have been Deep Neural Networks, Reinforcement learning and Generative Adversarial Networks (GAN).

  Medical Diagnostics is where AI is making major inroads. The Profound platform of Zebra Medical Vision has a 90 per cent accurate diagnostic prediction of a large number of diseases like cancers, osteoporosis, cardio- vascular disorders etc. along with medical imaging like CT scans and mammographs. There has also been widespread use of AI based Clinical Decision Support (CDS) tools to help care providers decide on the best line of treatment for each individual patient, as well new drug developments.

  The financial sector has also seen the rapid integration of AI based systems for credit ratings, risk assessment, loan disbursement, compliance, fraud detection and data extraction functions. It can be said that there have been very few industries or sectors where AI based learning systems have not been deployed.

One of the major requirements of AI based learning systems is access to a vast quantity of data sets that are properly annotated. This places an enormous burden on human resources for annotation, provided that relevant data set is available. In addition, a suitable algorithm along with necessary computational power is essential for developing an effective AI based learning system.

- ***NLP:*** One of the biggest breakthroughs in NLP is the use of *Transfer Learning* to train AI platforms with minimum training data sets. *Transfer Learning* is the process of using pre trained complex Deep Learning models and thereafter tweaking them to perform NLP based specific tasks.



Source: Analytics Vidhya

The popular Transfer Learning model for NLP is the Universal Language Model Fine-Tuning for text Classification (ULMFiT) which uses the pre trained language model from Wikitext 103 labelled data set.

The major breakthrough in NLP occurs when the intelligent machine is able to understand the context of words in different day to day spoken sentences and is able to respond in a question answer format in real time such that, the human at the other end of the telephone is unable to distinguish whether the call has been made by a human or machine. This was recently demonstrated by Sundar Pichai, CEO of Google in May 2018 when the Google Assistant using its proprietary AI system Google Duplex, made an appointment for a haircut with a real world salon.[8] Similarly, Facebook is working on its PyText system for enhanced NLP features with some very promising results.

Embedded for language Models (ELMo) is a deep contextual language model which uses language models to create embedding of each spoken word and understands the context of the word when used in a sentence. ELMo is an example of the transfer learning model which can drastically reduce the learning curve of a new NLP based intelligent agent.

The use of NLP based intelligent agents is almost limitless. They can be used in call centres, as digital assistants, in voice recognition systems, etc. On the other hand, fake voice overs of famous personalities can also be created by the same techniques.

- **Computer Vision:** Advances in image recognition, enhancement and reconstruction have been at the fore front of the AI based technologies basket primarily due to the availability of vast quantities of image related data sets like Imagenet[9] and the immense interest in the technology shown by innumerable industries. The implementation of deep learning neural networks has revolutionised the field of computer vision in more than one ways. Fast.ai's[10] computer vision model was trained in just 18 minutes with an accuracy of 93 per cent, at the extremely low cost of $ 40.00.

  Edge computing is a technique for analysing sensor generated data at the sensor location rather than accessing it from cloud. The AI system uses the cloud to improve upon its detection capabilities but analyses the data in real time, as it is being generated from the sensor. This not only reduces the latency time for analysing image/video data but is also extremely important in autonomous vehicles, which have to rely on real time analysis of the environment for safety and other reasons.

  Object Recognition in a Point Cloud is a method in which a three dimensional bounded space (cloud) is defined to the intelligent agent. The agent thereafter identifies and tracks all objects present inside this three dimensional space. The above technique is extremely useful for monitoring and tracking of assets, pilferage detection, classification of objects, etc. and has use in a number of industries ranging from construction sites to sensitive locations.

Merger reality is an enhanced technique over virtual reality which provides better environmental perception, updates the environmental picture based on eye and body movement and can be effectively used for navigation and guidance in difficult and hazardous locations like nuclear hazard sites, underwater caves, tunnels, etc.

Instance segmentation carries out object identification and analysis based on each constituent pixel of that object, while semantic segmentation does grouping at an object level. Together semantic and instance segmentation can be used to undertake image analysis of vast areas in real time by using semantic segmentation for identifying different objects and instance segmentation for the subsequent detailed analysis of each object.

- **Autonomous Vehicles:** There has been a lot of excitement and speculation concerning availability of fully autonomous driverless cars in the next few years, with Uber stating that bulk of cars available in 2030 will be driverless. A large number of companies including Google and Baidu are investing heavily in the autonomous vehicle technology.

  However, experts feel that a lot of developmental work is yet to be done before a fully automated vehicle without steering wheel and pedals is mass produced and hits the road. The via media of using technology to make driving more accessible, safe and comfortable to include piloted driving, traffic jam assist, automated parking, intelligent drive, etc. is likely to be the intermediate stage between a human driven and driverless land vehicle.

  The manufacture of fully autonomous fast moving aerial vehicles like fighter aircrafts and commercial planes is yet to be realised, because of the fast changing environment, decision making and execution in real time owing to the polynomial rising complexity of the problem. However, the game changers in aerial autonomous technology have been the rotary winged aircraft, especially quadcopters and drones. Recently, Boeing has announced the development of a fully autonomous carrier jet aircraft for the US Navy, MQ 25.[11]

A large number of autonomous helicopters and quadcopters have been developed with in- built AI chips that can have an endurance of as much as six hours and carry out multiple tasks ranging from terrain mapping, crop surveillance, object tracking, photography, etc.

Advancements have also been made in developing autonomous underwater vehicles especially for hydrographic surveys and underwater cable and pipelines inspection, etc.

- **Robotics:** Major advancements in industrial robots pertain to improvements in various sensors required for sensing the environment. Measuring the pressure applied by the effectors was a major challenge area, which has seen remarkable improvements by the use of tactile skin which utilises the variations in the flow of light through the object to detect the amount of pressure applied by the effector on it.

  Another major advancement has been seen in the field of collaborative robots or cobots which work in tandem to perform a variety of tasks ranging from packaging and palletisation, injection moulding, quality inspection, pick and place, etc.

  Robots are increasingly being used to replace labour in hazardous tasks and areas. The Rio Tinto group launched their Mine of the Future[12] programme in 2008. This has resulted in a centralised AI driven single Operations Centre at Perth with a large volume of work like autonomous haulage, drilling, working of various types of machinery, etc. being carried out by robots.

  There have also been significant developments in humanoid robots which walk, talk and mimic human gestures and movements. In August 2018, Professor Hiroshi Ishiguro of Osaka University and his team developed a number of robots with motion, gaze, speech and emotion features to mimic the verbal as well as non verbal communication patterns of humans. The humanoid robot "Erica" became an instant hit and launched its own YouTube channel in April 2019.[13] The team also developed a group of conversational social robots named "CommUs".

In the field of mobility robotics, a large number of robots which mimic humans, animals, insects and wheel/tracked based vehicles, have been developed. Boston Dynamics[14] has produced an impressive array of multi utility mobility robots ranging from: Spot (small dog shaped, capable of climbing stairs, lifting objects); Atlas (75 kg, 1.5 metre humanoid, capable of carrying 11 kg payload, backflip and negotiating multiple obstacles); Big Dog (used for rough terrain mobility); and Wild Cat (world's fastest quadrupled robot having top speed of 32 kmph).

- **Optimising and Decision-Making:** AI is increasingly being used for improving the quality of decisions as well as assisting leaders in making optimum decision-making by selecting options, reducing information overload and using collaborative decision making models.

  Intelligent Decision Support Systems (IDSS) are increasingly being used in finance, health care, marketing, commerce, command and control and cyber security systems.[15] A decision making process consists of four phases: Intelligence (used for gathering information and understanding the problem); design (used for identifying criteria, modelling of the problem and analysing alternatives/options); choice (comparing and analysing alternatives/options to arrive at the best solution); and implementation (executing the alternative/option and obtaining feedback from it).

  Most of the AI driven work in decision making revolves around Business Intelligence (BI) and Analytics. Some of the major challenges facing real world complex decisions are: High levels of uncertainty due to the partially observable environment; widely distributed and unstructured data; too many variables in decision making loop; and high risk potential of sub optimum decision. The ideal IDSS should learn from experience, reduce ambiguity, respond quickly to fast changing situations, apply correct knowledge and generate workable options.

  AI based decision support systems have been successfully used in the transportation sector for improving efficiency in terms of cost, time, assets and medium (road, rail, air, sea) as well as road planning, traffic condition prediction and reducing congestion. Artificial Neural Networks (ANN), Genetic Algorithms (GA), Simulated Annealing (SA), Artificial Immune System (AIS), Ant Colony Optimiser (ACO), Bee Colony Optimiser (BCO) and Fuzzy logic Model (FLM) are some of the tools utilised in transportation based IDSS.[16]

Stumbling Blocks of AI: Rapid advances in global telecommunication networks, high speed data transfer, storage, cloud and computing resources in the past two decades, have led to the emergence of an eco-system which was just right for the explosive growth of AI based systems and technologies. However, the technology is yet to transform itself into the genie capable of knowing all and doing all and a single generalised AI system is more of a dream than reality.

- **Lack of Annotated and Clean Data Sets:** AI systems require a large quantity of annotated and clean data sets especially during the training phase. Most of the data being generated by organisations is not properly structured or annotated making it unsuitable for AI based systems. The data preparation and engineering tasks represents 80 per cent of the time consumed in most AI and machine learning projects.[17] One of the major problems in fielding AI systems is the non-availability of data, especially in developing countries like India.
- **Bias in Data and Algorithm:** Training an AI system is one of the most critical tasks which heavily depends on the quantity and quality of data collected. An insufficient quantity of data or a data set which has been collected with an introduced bias (intentional or unintentional) towards a particular gender, race, religion, society, country, etc. may result in skewed AI results could cause serious real world problems. One of the major problems being faced is that data collection, cleaning and annotation is one of the major expenditure areas for a company providing customised AI solutions to its clients. Any shortcuts taken during this process will result in faulty training being provided to the AI system with drastic consequences.

Also, AI systems need to undergo extensive pre-release trials to ensure that there are no biases and problems with the algorithm before being fielded. Sometimes, due to monetary and time criticality reasons, the same are not carried out in letter and spirit. An unintentional introduction of bias in a data set for medical diagnostics as for example not collecting blood samples from the complete cross section of a given population base, could result in a diagnosis which might not be applicable for a community, whose typical blood composition has not been represented in that data set. In some AI systems the images corresponding to CEO, doctors and engineers are male representations, while those corresponding to nurses and teachers are female representations. Recently Amazon did away with its AI based recruitment system after it was discovered that it was discriminating against women.[18]

Biases can also be introduced in the algorithm when we try to break a complex real world problem into doable AI based algorithms. The problem of introducing bias in an AI system is that over a period of time the effect of bias gets amplified in the output.

- **Black Box Syndrome:** AI systems take input from the sensors and produce an output to the actuator. The internal processing of information to arrive at the output is unknown, as it represents an iterative mechanism of probability and utility driven algorithm, which is learnt by the system based on its initial learning data set and subsequently followed by inputs received from the environment.

  Nowadays, more and more critical decisions are being taken based on AI system generated output. Most of the credit card and financial companies sanction loans and mortgages based on the AI generated ratings and approvals of persons and businesses. In addition, AI platforms are increasingly being used by the judiciary to sanction bail bonds and decide on prison sentences of convicts. There is thus a growing concern that the decisions taken by AI systems should have an 'explainability' factor to explain the flow and nature of processing the input to arrive at a given output.

- **Non Generalised Approach: One system for one problem:** The present breakthroughs are happening in the field of narrow AI which translates to different AI models and systems for different types of problems. For example, convoluted neural networks are more suited for performing image interpretation tasks while recurrent neural networks are suited for audio and text interpretation tasks. This increases the time, cost and resources needed for fielding different and unique AI based systems, across the entire length and breadth of multiple industries and fields. A large volume of research is currently being carried out in the field of Artificial General Intelligence (AGI), which revolves around the building of intelligent agents capable of performing multiple tasks like humans. Rey Kurzweil in his book The Singularity is Near[19] has predicted that AGI would be possible by 2045.
- **Limitations of Algorithmic Decision Making Systems:** AI based systems are increasingly being used to make decisions concerning humans like extending credit lines, acceptance or rejection of visa applications, social state modelling based on comments and usage of social media platforms, etc. The results produced by AI system make two important assumptions. First, human conduct is consistent over a period of time and second, if sufficient data is available, human behaviour can be predicted. People tend to rely more on AI produced decisions, as it is generally perceived that these decisions are more transparent (absence of any ulterior motive by the machine) and more efficient (faster and more accurate decision making). However, the opacity of the process (black box syndrome) coupled sometimes with flawed algorithms or inconsistencies in the training process and data set can lead to faulty decisions.

  There is therefore merit in the argument that critical decisions like medical diagnoses and treatment etc. which can have a major impact on a person or entity need to be reviewed by humans, as a second line of decision making prior to finalising them.
- **Multi-disciplinary Field:** AI is a highly multidisciplinary field involving not only mathematics and computer science but also psychology, philosophy, linguistic studies, economics, etc. Since

> AI based results are greatly influenced by the training data set and the ability of the algorithm to capture the essence of a given problem and thereafter convert it into machine understandable mathematical solutions, a small error or bias in either the data collection and annotation or algorithm can lead to compounded errors over a period of time. It is feared that some of the AI systems developed in haste were more or less based on the efforts of only mathematicians and computer scientists with little, or no contribution, from other relevant professionals.

Ethical AI: There is a growing concern within the AI community that use of AI should be strictly for the greater good of mankind as it is a powerful tool and a double edged weapon capable of causing immense harm and destruction. The UNESCO has raised a red flag on numerous ethical issues concerning use of AI like video surveillance, facial recognition, behaviour prediction (terrorist and criminal behaviour profiling), racial profiling and one's sexual orientation.[20] It voiced its concerns during the high level dialogue at the World Summit of Information Society (WSIS) 2019 on April 10, 2019 and stressed that emerging technologies need to be developed with a respect for universal ethical principles and fundamental human rights. Post a series of meetings, the Extended Working Group on Ethics of AI of the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) gave its recommendation to UNESCO, with regard to the necessity of a standard- setting instrument regarding the ethics of AI.[21]

Institutions like IEEE[22] have enumerated their own code of ethics along with technology giants like Google, Facebook and Microsoft. The Future of Life Institute is a non-profit organisation founded by MIT cosmologist Max Tegmark, Skype co-founder Jaan Tallin and Deep Mind researcher Viktoriya Karakovnahas. The institute has come out with an elaborate AI code of ethics known as Asilomar AI Principles which have been endorsed by famous personalities like Elon Musk and Stephen Hawking.[23]

Key Takeaways: The field of AI is different from the traditional means of arriving at automated results. Mathematical models are used in the traditional methods to arrive at outputs from given inputs with each step of processing intimately known to the system designer. AI on the other hand is a data driven technology where an algorithm provides the means to the intelligent machine, to process data and arrive at output. The machine thereafter self learns from the huge quantities of labelled data sets to improve its performance and subsequently uses real world data sets to continuously adapt and produce outputs. The steps involved from reaching the output from input cannot be explicitly laid out. The quality of output is an indicator of the efficiency of the algorithm, quality and quantity of input data and the power of the computational engine. Some major takeaways regarding AI based intelligent agents are:

- AI systems are heavily dependent on the quantity and quality of training data. For accurate and efficient outputs the data set needs to be without bias, in a large quantity with all the relevant attributes required for producing the output.
- AI systems are best suited to produce results for NP hard problems. Here, deep neural networks are used to construct Bayesian tree structures with probability distributions so that good decisions (not 100 per cent accurate decisions) are made in finite and workable time frames.
- It is always better to divide a complex problem into a large number of small doable problems which can be accurately modelled mathematically.
- The mathematical algorithm construct and the type of processing (convoluted neural network, recurrent neural network, GAN, etc.) of information is critical for arriving at accurate results.
- Considerable progress has been made in the fields of machine learning (single layered AI systems), neural networks (which enable more accurate results for complex problems and assist in contextual learning) as well as in transfer learning (helps in faster training of AI systems with minimum requirement of data sets).
- Each problem has a unique AI solution. Presently there are no generalised AI systems available.
- AI systems are efficient and scalable. Once an AI system has matured, its efficiency increases exponentially to surpass human

capability in that sphere and it can be replicated with relatively minimal expenditure on resources.

- Research in AI based technologies is globally shared and disseminated, with researchers exchanging notes as well as source codes on multiple websites and platforms.
- A multi-disciplinary approach is necessary while formulating complex AI systems. Detailed pre fielding tests and human impact assessments need to be conducted prior to fielding AI systems.
- Complex AI systems dealing with human safety and health should always have human monitoring and control interface.
- Developmental work in AI, which is a dual use technology (can be used for benefit as well as harm to humanity) should be regulated by universal ethical code of conduct.

AI in Warfare

Introduction: The United States DARPA has done seminal work in the field of AI and has been the incubator for a number of ICT related technologies including internet and world wide web. The world is witnessing a rapid transition from the industrial era to the information era war fighting, where the boundaries between war and no war have blurred and it can be safely assumed that a large number of nations have to be prepared to fight this battle, day in and day out without any formal declaration or cessation of hostilities. Use of AI in warfare is not only restricted to fielding of autonomous lethal weapon systems or remote piloted mobility platforms but this revolutionary technology can also be applied towards: improving defence preparedness, formulating better decisions in the fog of war, optimising logistic solutions; improving integration of intelligence; operations; logistics; command and control of geographically spread out forces; and the various business processes being utilised day in and day out by modern militaries, across the globe. In a study conducted by the BELFER-Centre of Harvard Kennedy School for US Intelligence Advanced Research Projects Activity (IARPA), the authors state that "AI is likely to be a transformative military technology, on a par with the invention of aircraft and nuclear weapons."[24]

In 2018, the US DoD released its AI strategy.[25] The strategy requires the DoD to accelerate the adoption of AI and harness its potential to transform all functions of the department positively. Towards this end, the Joint AI Centre (JAIC) will take the lead in developing shared data, reusable tools, frameworks and standards, cloud and edge services to usher in transformative AI. The strategy further adds that "we will use AI-enabled information, tools, and systems to empower, not replace, those who serve." Four strategic areas namely improving situational awareness and decision making, increasing safety of operating equipment, implementing predictive maintenance and supply and streamlining business process have been outlined in the strategy. The strategy lays emphasis on the fact that the AI used by the DoD will be lawful and ethical.

AI in Intelligence related activities: There are four types of intelligence related tasks in military. These include: the support for situational awareness tasks which range from Intelligence Preparation of the Battlefield (IPB); formulation of various intelligence related databases (terrain, equipment, population, personalities, going, infrastructure, etc.); ascertaining adversaries Order of Battle (OOB) to include force structures, dispositions, command and control hierarchy, morale of troops, etc.; and scenario painting/threat analysis. The second task is to provide commanders with indicators and warnings of adversary's likely plans, actions and mind set, etc. Third is to conduct intelligence surveillance and reconnaissance (satellite and aerial imagery, signal intelligence, open source intelligence, human intelligence tasks, population and resource monitoring, post-strike damage assessment, etc.) and lastly the counter intelligence tasks. AI is ideally suited for this and can be extensively utilised in all the above tasks.

In the industrial age, the majority of sources which could result in useful intelligence were in the classified and internal domain of various headquarters/ministries/offices. In the present age, the majority of these sources lie in the unclassified and open domain. The challenge is the sheer volume, velocity and complexity of data which needs to be analysed in quick time to extract actionable intelligence. AI especially Machine Learning is the ideal candidate for performing such kinds of tasks.

Already, major countries like US and China are employing AI platforms for a large number of intelligence related tasks especially relating to imagery analysis, facial recognition, NLP based contextual learning platforms, signals intelligence and open source intelligence.

AI in Military Operations: The United Kingdom (UK) Doctrine on Land Operations[26] states that "all armed conflict is essentially **adversarial**, **human** (involving friction, uncertainty, violence and stress) and **political**." It goes on to state that since the conflict is essentially human, it is influenced by human behaviour, emotions and capabilities and cannot be reduced to scientific templates. It relies on initiative, enterprise and intelligence. In the age of AI, we need to ask ourselves whether the above statement really hold absolutely true or there are ways and means to remove/ replace the human in the conflict.

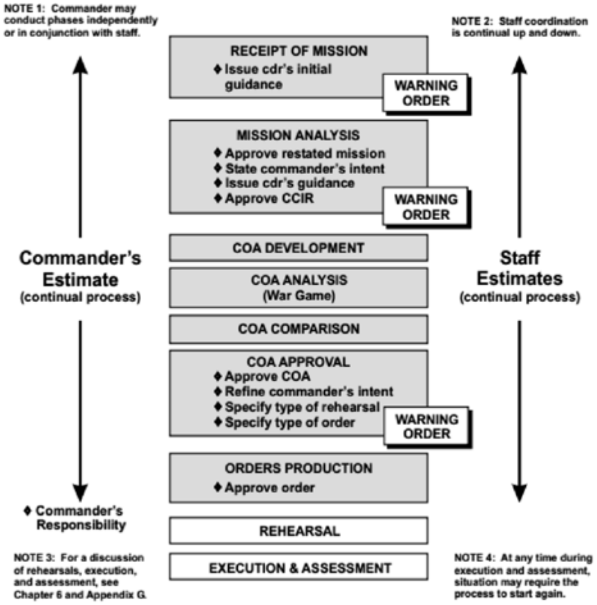
The operational aspects of warfare can be broken down into five major components. First, **military decision making** which can be strategic, operational or tactical. Second, **information operations** which is essentially psychological warfare, cyber warfare and electronic warfare. Third, **command and control** which revolves around combat structures and communications. Fourth, **combat power** which can be aerial, land and sea based platforms coupled with firepower and engineer elements and lastly **strategic forces** which can either be special operations forces or nuclear forces.

- **AI in Military Decision Making:** Military decision making is a very challenging and complex task as decision makers have to make decisions based on partially available information (fog of war), generate one of a kind unique multiple solutions (options) for a complex problem, using multiple inputs from a variety of sensors (information overload) in a strictly time bound manner (faster OODA loop) which can have far reaching strategic ramifications, that can threaten the very existence of a nation state. Traditionally, humans and machines have performed this task in water tight compartments with machines generating fixed outputs irrespective of the current state and type of operation.

  Daniel Kahneman[27] has classified human decision making into two types. Type 1 decision making is intuitive and automatic, which is a rule of thumb quick fix solution to a problem by simplification and lays major emphasis on past experiences and heuristic. Type 2 decision making is a deliberate and controlled process which is rule based, but entails more effort and is comparatively slower than the Type 1 decision making process. Humans, generally resort to Type 1 decision making which has more bias and errors of judgement compared to Type 2 decision making.

Militaries generally rely on an iterative decision making process known as Military Decision Making Process (MDMP) which is detailed, deliberate, sequential and time consuming. The process essentially revolves around evaluating a number of own and enemy's courses of actions (COA) to evolve the operational plan. However, this approach suffers from being extremely resource and time intensive and can also lead to flawed decision making assuming that all possible courses of actions have been studied and resolved.

Military Decision Making Process


NOTE 1: Commander may conduct phases independently or in conjunction with staff.
NOTE 2: Staff coordination is continual up and down.
RECEIPT OF MISSION
♦ Issue cdr's initial guidance
WARNING ORDER
MISSION ANALYSIS
♦ Approve restated mission
♦ State commander's intent
♦ Issue cdr's guidance
♦ Approve CCIR
WARNING ORDER
COA DEVELOPMENT
COA ANALYSIS (War Game)
COA COMPARISON
COA APPROVAL
♦ Approve COA
♦ Refine commander's intent
♦ Specify type of rehearsal
♦ Specify type of order
WARNING ORDER
ORDERS PRODUCTION
♦ Approve order
REHEARSAL
EXECUTION & ASSESSMENT
Commander's Estimate (continual process)
Staff Estimates (continual process)
♦ Commander's Responsibility
NOTE 3: For a discussion of rehearsals, execution, and assessment, see Chapter 6 and Appendix G.
NOTE 4: At any time during execution and assessment, situation may require the process to start again.

Source: Australian Army Field Manual 101-5

Karel Van den Bosch and Adelbart Bronkhorst from TNO,[28] an independent think tank in the Netherlands, argue that AI based Intelligent Decision Support Systems (IDSS) can support the military decision maker by collecting and analysing information, detecting patterns in data, checking hypotheses and evaluating CoAs. These can respond to new and uncertain situations and can perform cognition functions like knowledge representation, intent recognition, machine learning, automated inference and data mining. However, due to the complexity of problems, uncertainty of information and implication of decision, the AI based IDSS should not function autonomously but interact closely with humans evolving decisions by means of a step by step approach in order to build trust and cooperation between the human and machine. This can be done when the machine adapts itself dynamically to the decision maker by taking into consideration his objectives, preferences and biases and offers explanations, for arriving at its inferences, thus improving faith and trust in the IDSS over a period of time.

- **AI in Information Operations:** In today's information driven world, the role of information in military operations is increasing day by day. Since a large portion of information operations are technology driven, there is an enormous scope for AI driven solutions in this field. Most of present day surveillance revolves around an analysis of digital meta data in real time. According to a recent study, the world's digital data doubles every two years and by 2020 it will be 44 zettabytes or 44 trillion gigabytes.[29] The analysis of this magnitude of data within a reasonable time frame, can only be performed by AI based systems. As the data size increases, the capability of data analysis will be restricted to only a handful of niche countries who have invested heavily in AI based R&D and have a viable ecosystem for assimilating, analysing and disseminating of digital data intelligence. The rest of the world will have to rely on these countries for intelligence, which is likely to give rise to a new and emerging power balance in the world order.
    - **AI in Psychological Operations:** In February 2017, Oxford University conducted a workshop to forecast, prevent and

mitigate the harmful effects of malicious use of AI. The findings of the workshop[30] throw light on a number of important issues, that are mentioned below.

- Present day AI based neural networks are able to identify and categorise images with an accuracy of 98 per cent which is greater that the human accuracy of 95 per cent. Generation of synthetic images, texts and audio (deep fake) has also reached a level where it has become increasingly difficult to distinguish between an original and fake.
- Use of AI in surveillance (deep analysis of mass data consisting of images, texts, geo locations, audio, etc.); persuasion (creating targeted propaganda/narrative); and deception (deep fake), has radically changed the scope and depth of psychological operations.
- Apart from the above, AI systems can be used to deeply analyse human behaviours including emotions, moods, beliefs and sentiments to target people when they are extremely vulnerable and susceptible to manipulative messaging. The case of Cambridge Analytica and the Democratic National Committee (DNC) hacks are just the tip of the iceberg.

- **AI in Cyber Warfare:** The AI attributes of efficiency, scalability and diffusion coupled with anonymity and autonomy may result in a plethora of cyber threats ranging from: new age social engineered spear phishing attacks (say realistic images, voice of friends in distress for targeting of high value individuals); automated AI hacking tools (for targeted vulnerability detection and hacking of applications and systems (hardware as well as software) of individuals as well as organisations); human like Denial of Service Attacks (targeting ATMs on salary day etc.); and exploiting AI based cyber defence systems. On the other hand, use of AI to access network behaviour and track threat activity in order to warn administrators of impending cyber-attacks will support a stronger cyber security posture and have a dynamic threat management and mitigation system, capable of adapting the cyber defence structures based on the evolving threat landscape. The availability of a large number of free to use AI based malicious codes across the entire cyberspace ecosystem, helps to enhance the sophistication of attacks by individuals and organisations with limited resources and skill sets.

  - **AI in Electronic Warfare (EW):** EW primarily involves exploiting the EM spectrum for own use while successfully denying it to the adversary, to gain an information advantage in space and time. One of the biggest challenges in EW systems is the real time analysis of the huge quantity of data/ intercepts from multiple sources ranging from radio and satellite receivers to radars, in order to arrive at an electronic intelligence picture of the adversary, based on which future CoAs are decided by commanders. AI, especially deep neural networks, are ideally suited for such types of tasks. In addition, synthesis of information from multiple sources ranging from EW intelligence, human intelligence, imagery and open source intelligence, would greatly assist the commanders in reducing the fog of the war and lead to a better understanding of the battle picture, including threat assessment and the response mechanism.

- **AI in Military Command and Control:** Over the ages military command and control structures have evolved from the strictly water tight and hierarchical to more interdependent and flat ones. Command and control in military is extremely important as strict levels of command in units and sub units are put in place on the basis of which of these platforms/elements are controlled by the authorised person. The overall aim is the cohesive and coordinated use of maximum combat power to achieve the desired objective. Major components in military command and control are decision making and communication.

Communications empower military commanders by allowing them to exercise command and control over multiple and varied units which are geographically spread out. The quality of military communication network, in terms of its geographical reach, peak data handling capacity, up time and guaranteed quality of service, secrecy, resilience and ability to integrate multiple communication devices and media seamlessly, has a direct bearing on the operational efficiency and reach of any battle force. AI based systems in military communication networks are used for congestion control, dynamic bandwidth allocation, traffic routing and rerouting, threat detection and mitigation and network health monitoring and diagnostics.

One of the major challenges facing a military commander is the formulation of Common Operating Picture (COP) and its dissemination to the entire battle force. Formulation of the COP becomes more difficult in case there is limited or uncertain information about the enemy, there is a large spread and number of own units and a large volume of data is flowing in from multiple agencies and sensors. AI based systems can be used to dynamically generate and evolve a COP by means of human intervention.

DARPA in 2013 developed and introduced the Deep Green (DG), an AI based tactical command and control system, to the US Army. The DG is capable of generating and analysing multiple CoAs based on enemy's intent and actions thus allowing tactical commanders to take high quality decisions in quick time, which in turn, results in faster generation of OODA loop and translates into increased combat potential. DARPA is presently carrying out research on Real time Adversarial Intelligence and Decision making (RAID) systems by using predictive analysis, AI and simulations to analyse large scale operational adversarial actions.[31]

- **AI in Combat Platforms/Systems:** Most AI technology is dual use wherein it can easily be adapted for military use. The primary areas of focus are robotics, autonomous weapon platforms, which are capable of carrying out lethal attacks without human intervention and swarm systems, comprising of multiple autonomous mobile devices capable of evading known deterrence systems and shields.

The world's expenditure on military robotics (including unmanned aerial, ground and sea borne vehicles) tripled from $2.4

billion in 2000, to $7.5 billion in 2015 and is expected to reach $16.5 billion in 2025. This remarkable spend is taking place at a time when there is a steep decline in the cost of military robotic systems. The steep learning curve of military robotic systems based on deep neural networks coupled with increasing computational power and powerful algorithms, is facilitating the shift from remote controlled unmanned combat vehicles to autonomous unmanned combat vehicles, capable of taking intelligent decisions based on sensor inputs. This will lead to unmanned combat missions being preferred over manned combat missions, especially in situations of great risk. This will be followed by overcoming the size, weight, range and power constraints of present day robotic systems, just like smart phones have become more compact, powerful, long lasting and cheap.

There are clear indicators to suggest that most militaries around the globe would progress to lethal autonomous weapon systems. A $35, Rasberry Pi based AI system developed by a doctoral student from the University of Cincinnati was able to defeat a US Air Force trained pilot in combat simulation in June 2016.[32] The Russian Military Industrial Committee has committed that 30 per cent of Russian combat power in 2030 will consist entirely of remote controlled and autonomous robotic platforms.[33]

The cost of a high end autonomous drone like a quadcopter is $1000. Over one million such drones can be purchased for the cost of one fighter aircraft. One of the major breakthroughs in swarm technology is the self-location and self-synchronisation capability of a large cluster of miniature drones. These abilities enable large numbers of fully autonomous platforms to perform a variety of tasks like deep area search and rescue missions, decoy and deception tasks, fail modern sensors and interception systems and act as weapon platforms. In February 2019, the UK Defence Secretary declared that “Swarm Squadrons” would be deployed by the British Armed Forces in the coming years.[34] DARPA is also developing a range of combat swarm platforms like *Project Gremlin* which are micro drones of the shape and size of missiles, to be ejected from aircraft for performing a range of combat missions and capable of aerial recovery, post mission. Each gremlin would have the capability of carrying out 20 missions. The first test flight of the system is expected by end of 2019.[35] To ensure survivability and operational capability in a combat environment in the midst of adversary's active aerial and EW activity, DARPA is developing the concept of Collaborative Operations in Denial Environment (CODE) wherein a squad of drones would adapt and operate in such a hazardous environment.

AI in Military Logistics: Military logistic functions are extremely challenging and unique from day to day logistic operations carried out by most multinational companies. First, there is the element of uncertainty as logistical tasks during combat mostly evolve at the last moment and are frequently changed, depending on the current battle picture and plans. Second, the logistics have to be extremely flexible and responsive to cater for last minute changes, damage to stocks, men and material and change in transportation means and modes. Third, logistic plans are rarely repeated and have to be unique for each and every operational task. Fourth, the operating environment is hostile and susceptible to rapid degradation and destruction and finally, the necessity of highly efficient and time critical logistic chains and processes.

AI can be utilised in all aspects of military logistics ranging from stocking and inventory management, supply chain management, preventive maintenance, medical and casualty evacuation, transportation including use of driverless convoys and formulation of logistic plans and orders.

A cloud based data service and repository platform is essential for carrying out AI based system operations. First, the cloud ensures that all data generated by any military platform, personnel or organisation, gets uploaded and stored wherein it can be utilised subsequently without getting lost or misplaced. It is also easier to ensure centralised backup of data when it is stored on the cloud. Second, since data is one of the key components of any AI driven system, accessing it from the cloud is easier and simpler. Lastly, uploaded data can be utilised to train and improve the efficiency of a number of AI platforms. The US DoD's Joint Enterprise Defence Infrastructure (JEDI) has floated a tender of $10 billion to upgrade the department's cloud services in order to provide enterprise level IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) services globally. The contract has been awarded to Microsoft in December 2019.[36]

Military Supply Chain management is a big opportunity area for employing AI solutions. This is primarily because individual stocking and supply of parts and equipment to ordnance echelons in the field can be carried out by the correct and timely interpretation of logistic data. The above helps to reduce dead stock, cuts down inefficiencies in stock management, reduces time required for movement of parts and equipment and helps in better inventory management and improvement of overall operational logistic efficiency.

Presently, the preventive maintenance of complex and costly combat platforms like aircrafts, ships, missile systems and armoured fighting vehicles is carried out on a fixed time schedule and involves replacing parts, lubrications and components after pre calculated operation time cycles. The Autonomic Logistics Infrastructure System (ALIS) of the F-35 fighter aircraft is an AI enabled, web and cloud based integrated information environment platform which provides each aircraft's health and maintenance condition to multiple users worldwide, to ensure more responsive and personalised preventive maintenance for each individual aircraft. This results in lower operating and maintenance costs and increases aircraft availability.

AI and Machine Learning (ML) can also be utilised for fraud detection which is a main area of concern amongst military contracting agencies, globally. This is primarily due to the huge volume of tenders being floated and multiple bids being posted in response to the tenders. The US Defence Logistics Agency (DLA), has recently identified around 350 suspicious business entities indulging in wrong business practices, after fielding an AI and ML based fraud tracking system.

Similarly, a number of medical wearables which track individual health and vitals have been developed, which when uploaded on the cloud, can lead to the early detection of disease, as well as medical decision making and treatment of combat injuries.

Use of autonomous/semi-autonomous vehicles is being actively explored for transportation of military equipment and supplies in combat zones as they would enable better turnaround times, as well as reduce overall driver fatigue and vehicle wear and tear. In addition, autonomous flying vehicles like quadcopters can be utilised for delivering emergency supplies, medical aid, ammunitions, etc.

AI in Military Business Processes: Like any other business conglomerate, the defence forces have a large number of business processes ranging from human resource (HR), planning, procurement, strategic communication, training, administration and discipline, movement and transportation functions. Most of these business processes can be optimised by using commercially available AI technology and solutions.

One of the biggest advantages of AI based technology is that it can easily replace the human workforce employed on tasks which are repetitive and provide a fully observable environment with comparatively less uncertainty. Some tasks like call centre operations, clerical and personal assistance and store keeping can be easily automated, relieving human workforce, which can be employed for more highly skilled tasks.

AI coupled with cloud based architecture can empower today's knowledge worker and enhance efficiency, by not only retrieving relevant information but also by generating multiple options and evaluating decisions. Savings in manpower can also be effected by automating workplaces and the introduction of robotic workers in static peace time locations like workshops, stores, cook houses etc.

Indian Initiative in AI

Introduction: It was in the nineties, that the government of India realised that a digital India strategy will go a long way, towards overcoming a large number of the hurdles facing the country such as corruption, red tape and slow delivery of services. Along with highways, sea ports, power plants and other infrastructure projects, there was a dire need to have a state of the art digital ecosystem which covered all the corners of the country and was capable of meeting the digital needs of each and every citizen. The initial projects were the railway reservation computerisation system and digitisation of land records. These were subsequently followed by provisioning of limited e-services to the citizens.

The national e-governance plan was initiated in 2006. It had 31 Mission Mode Projects (MMP) like agriculture, land records, health, education, passport, police, courts, municipality, commercial taxes, etc. In spite of making modest gains, the national e-governance plan suffered from major drawbacks like lack of integration between applications, limited re-engineering of processes and non-utilisation of emerging digital transformative technologies like mobile, cloud computing, etc.

In 2014, the e-Kranti national e-governance plan was launched with the vision of "Transforming e-governance for transforming governance". This truly transformative programme is based on 11 principles namely: transformation not translation; integrated and not individual services; mandatory Government Process Reengineering (GPR) in each MMP; ICT infrastructure on demand; cloud by default; mobile first; fast tracking approvals; mandating standards and protocols; language localisation; a national Geo-Spatial information System (GIS); and security and electronic data preservation. The number of MMPs have also been increased from 31 to 44.

Digital India is the overarching umbrella programme of the government covering all ministries and institutions and aimed at harmonising functions and responsibilities towards creation of a truly digital ecosystem for all. The Ministry of Electronics and Information Technology (MeitY) is the coordinating ministry for this programme. Digital India has nine pillars, i.e. Broadband Highways; Universal Access to Mobile Connectivity; Public Internet Access Programme; e-Governance; Reforming Government through Technology; e-Kranti – Electronic Delivery of Services; Information for All; Electronics Manufacturing; IT for Jobs; and Early Harvest Programmes.

National Digital Infrastructure: A nation-wide OFC coverage is a must when a country strives to build a state of art digital infrastructure. Till date there is no medium except OFC, which can carry high capacity highway standard bandwidth with an extremely high Quality of Service (QoS), along with a high degree of immunity against EM interference and eavesdropping.

On October 25, 2011, the Government of India (GOI) approved a National Optical Fibre Network (NOFN) to provide connectivity to 2,50,000 Gram Panchayats (GP) as part of rural connectivity project. Each GP services around 2.56 villages thus the aim was to provide broadband connectivity to almost 6,40,000 villages. Most of the private service providers were based around cities and towns as they had a higher subscriber density per km of OFC laid, giving them a profitable and viable revenue stream. Thus, broadband connectivity in villages was lacking which prompted the government to initiate this project. A special purpose vehicle, Bharat Broadband Network Limited (BBNL) was formed and the world's largest rural broadband project was initiated. As of July 11, 2019, a total of 3,48,161 km of OFC has been laid and 1,31,756 GPs connected.[37] This has truly revolutionised the rural digital connectivity and afforded immense opportunities for commerce, communication and education.

The real game changer in the Indian telecom sector took place in September 2016 when Reliance Industries launched Reliance Jio, their nationwide telephony services offering free calls and extremely low cheap broadband data rates. This was possible because Jio developed the complete ecosystem, including building an impressive pan India OFC network in record time and getting spectrum licences for all 22 circles of the country. Post launch of Jio, India became the world's largest data consuming nation. Six months after launch, the data consumption rose from 20 crore GB per month to 120 crore GB per month.

Another major game changer in the field of AI is 5G. There is no denying the fact that the 5G network in India needs to be implemented on a war footing. This is essential because all next generation applications and services will require a wireless backend which only 5G can provide. China is the leader in providing the 5G network backbone that is reliable and affordable. Huawei is the market leader in 5G network transmission systems. However, due to security concerns, the US and other developed nations have blocked the entry of Huawei into their countries. The world is watching India as its geographical size as well as the size of its internet population constitutes almost one third of the global wireless internet demand. One thing is certain, India needs the fast track implementation of 5G technology at competitive rates to usher the AI revolution and provide #AIForAll.

National Digital Databases: Having a digital dataset is the first step in implementing large scale AI systems. Thus, the importance of databases. As one of the most populous countries in the world which is also the largest user of social networks and generates the maximum data, the Indian data resource can be a major source of impactful data sets used for training the AI systems of the future. The Unique Identification Authority of India (UIDAI) is a statutory authority established under the provisions of the Aadhaar (targeted delivery of finance and other subsidies, benefits and services) Act 2016 with the aim to provide a unique and easily verifiable digital identity to all Indians. More than 200 million Aadhaar IDs have been issued till date.

The National Data Sharing and Accessibility Policy (NDSAP)[38] was formulated in 2012 and governs the ways and means by which the non-sensitive data generated by various organisations and institutions in the country can be used by the general public for scientific, economic and developmental purposes. The Open Government Data (OGD) platform (data.gov.in) is a recent government initiative to create an open data ecosystem in the country. The various government departments and organisations publish their data sets as SaaS, in open formats for free public use. The platform has about three lakh data sets under 7,583 catalogues.[39]

Education: As per World Economic Forum report of 2016, India has the second largest number of Science, Technology, Engineering and Maths (STEM) graduates (2.6 million) in the world. However, when we compare the number of science and technology researchers per 1 million population, India had 216 researchers in 2015, compared to China which had 1205 researchers in 2016. The US had 4256 researchers in 2016 while the UK had 4391 researchers.[40]

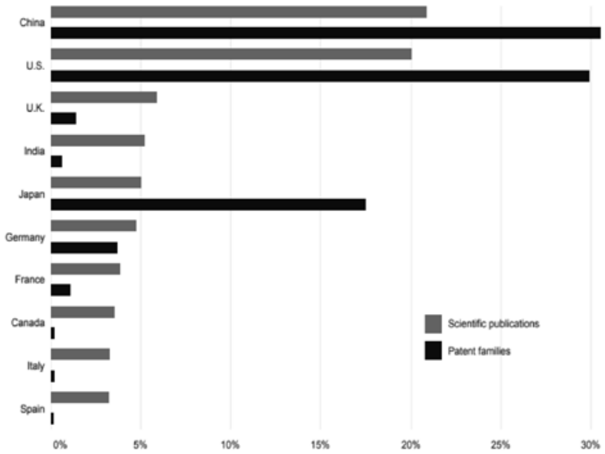
Governmental funding in the education sector has witnessed a downward trend till 2020, which is not conducive for developing high end niche technology sectors like AI. In 2013-14, the GOI had allocated 4.13 per cent of the GDP to education which still was less compared to the spending by developed countries like UK (5.68 per cent) and USA (5.22 per cent).[41] In the budget of 2019, 3.4 per cent of GDP amounting to Rs 93,847.64 crores was allocated for education of which Rs 37,461.01 crore has been allocated for higher education. In 2020, the government took corrective steps by increasing the allocation for education to Rs 99,311,52 crore and on higher education to Rs 39,466.52 crore. The budget for the Indian Institutes of Technology (IIT) has witnessed a drop from Rs 8,337.21 crore in 2017-18 to Rs 6,326 crore in 2018-19 to Rs 6,223.02 crore in 2019-20. It has been increased to Rs 7332 crore in 2020.

Research and Development: As per GOI report "Educational Statistics at a Glance" 2018, a total of 127,000 PhD researchers were enrolled in 2015-16, of which 24.16 per cent were in Engineering and Technology, 2.9 per cent in IT and computers and 26.25 per cent in Science.[42]

The World Intellectual Property Organisation (WIPO) published a report titled "Technology Trends 2019: Artificial Intelligence",[43] detailing on the results of the exhaustive research on AI from three angles, namely techniques like machine learning, etc., applications like NLP, etc. and fields like medical, transportation, etc. The majority of the analysis in the report has been based on patent analysis, which is an excellent measure of the changing technology trends over time. Since AI emerged as a discipline in the 1950s, around 3,40,000 patents and 1.6 million scientific publications have been generated in this field. What is notable is that more than half of these have been generated post 2013. In the same time period, there has been a major shift from theory to practice, as the ratio of scientific publication to patent has decreased from 8:1 in 2010 to 3:1 in 2016. Machine learning is the most dominating AI technique with more than 40 per cent AI related patents. Computer vision which also includes image recognition is the major application with 48 per cent of the patents filed. Telecommunication (15 per cent patent filing), transportation (15 per cent patent filing) and medical (12 per cent patent filing) are the top three fields where AI is being incorporated in a big way. Companies are filing far more patents than universities and public institutions. Among the top 30 contributors of AI related patents, 26 are companies. Of the top 20 companies who have filed for AI related patents, 12 are from Japan, three from USA and two from China. IBM has the largest portfolio of AI patents (8,290) followed by Microsoft (5,930). Among the universities, the Chinese universities dominate (17 of top 20 patent filing universities and 10 of top 20 scientific publications). The Chinese Academy of Science (CAS) tops the universities list with 2,500 patents and more than 20,000 scientific publications. China, USA and Japan account for 78 per cent of total patents filed and are the clear leaders in this field.

India has also emerged among the top 10 countries in the field of AI, both in terms of patents and scientific publications. It is in the top five in scientific publications related to computer vision, NLP, speech processes, predictive analysis, distributed AI and planning and scheduling. Among the patents filed for distributed AI, India ranks third.

Top 10 Countries in AI Related Patent Filing and Scientific Publications



Source: WIPO

AI based Industry: WIPO has also released its report on the "Global Innovation Index 2019" in collaboration with Cornell University and INSEAD.[44] According to the report, India remains the most innovative country in the central and south Asia region for 11th consecutive year, which is truly a remarkable achievement. Also, India has improved its rankings consistently from 81st in 2015 onwards to 52nd in 2019. Bangaluru, Mumbai and New Delhi are among the top 100 global clusters in science and technology and three Indian universities feature in the top 10 universities of middle income economies in the world.

As per a report by Analytical India,[45] the AI Industry in India grew from an annual revenue of $180 million in 2017 to $230 million in 2018. As per a report by Accenture, the Indian AI market will be $957 billion by 2035 which would be 15 per cent of the country's Gross Value Added (GVA) with an annual growth rate of 1.3 per cent. Infosys, Wipro and HCL technologies are among the top 10 AI driven companies in India which provide AI based products or services (chatbots, AI-powered visual search and recommendation engines). The number of pure AI companies in India are very few and presently, India's share in AI driven global analytics market is around 8 per cent.

The Ministry of Commerce and Industry has set up an AI Task Force to leverage AI for economic benefits, create policy and legal frameworks to accelerate deployment of AI technology and to provide five year horizon recommendations for government, industry and research programmes. In addition NITI Aayog has been tasked to formulate a national programme to develop research and development in niche technologies like AI and to formulate India's national strategy on AI.

The AI task Force in its report[46] has identified 10 AI empowered domains which are relevant for India namely: Manufacturing; Fintech; Health Care; Agriculture; Education; Retail/customer engagement; Aid for Differently Abled; environment; National Security; and Public Utility Services.

In February 2018, MeitY constituted four committees to explore different facets of AI.[47] These are: Platforms and data for AI; leveraging AI for identifying national mission in key sectors; mapping technological capabilities; key policy enablers required across sectors – skilling and re-skilling, R&D; and committee on cyber security, safety, legal and ethical issues. The reports from all the committees were submitted in July 2019 and are available in the public domain.

Conclusion

From its humble origins in the 1950s, AI as an emerging subject and technology has indeed reached commanding heights. Converting theory into practice would not have been possible without the concurrent developments in the fields of commercial grade off the shelf cheap processors and Graphic Processing Units (GPU), fielding of global internet, high speed large bandwidth data networks, global ICT companies with data generation and aggregation as primary source of revenue, cloud and exponential increase in memory capacities. It is almost surreal that all these concurrent technologies mushroomed and matured at the same time in order to usher in the AI revolution which is the ultimate saviour and knight in shining armour for solving all our problems and inefficiencies.

AI as a technology has the ability to touch and improve each and every portion of human endeavour. Be it engineering, medicine, legal, manufacturing, agriculture, transportation, planning, optimising, forecasting, meteorology – the list is endless. Thus, as the AI revolution gathers speed and momentum, tectonic shifts that will tear down structures, replace and create new jobs and change existing perceptions and beliefs, will take place. This revolutionary technology offers developing countries like India a relatively higher skill set in science and technology and an age dividend, which will be a golden opportunity to leap forward from a middle income economy to a developed economy.

The three essential ingredients for fielding world class AI systems are large data sets, accurate algorithms and high processing power. The AI ecosystem has to be developed as an all-encompassing cluster where highly trained professionals of diverse and multiple specialisations with exceptional skill sets have access to vast quantities of clean and annotated data sets and extremely high computational resources. Thus industry, education, research & development and digital infrastructure (data centres, cloud and high speed internet) have to coexist and cooperate in an environment where failures are accepted, government acts as facilitator and start ups are promoted and encouraged.

Handling and the safe keeping of large quantities of data is a major challenge which needs to be overcome. As a thumb rule, it can be safe to assume that no digital data is ever lost. Recent incidents of massive data thefts coupled with use of data to generate targeted ads to sway election results, has drawn the world community's attention towards this precious yet rarely understood commodity. Since, data is an artificial resource, each bit of it has to be attributed to someone and a value assigned to it. Till now, the technology savvy ICT companies had obtained access to large volume of user digital data, by ensuring that end user agreements were lengthy and confusing. In a nutshell they ensured that the user had given up all rights to the data generated by him. Governments and other organisations are now trying hard to curb this rampant practice. AI industry thrives when data is converged, clean and annotated. Data localisation affects the AI industry which is trying to find global solutions. However, the challenge for the governments is to tread a fine balance between requirements of the AI industry, data sovereignty and user digital privacy rights.

Most AI technologies are dual use technologies. Use of AI in warfighting is a fast developing field and autonomous vehicles like swarm drones, etc. and robotics are revolutionising the ways wars will be fought in the future. There is also a looming threat of military grade psychological weapons, with deep fake technology which will make it extremely difficult to segregate the true from the false and can radically change the cultural and societal norms of nation states. The military power balance will be greatly tilted in favour of countries employing large scale niche AI enabled technologies, thus sparking off a new technology driven arms race.

Use of facial recognition and meta data analysis have raised major privacy concerns which need to be addressed by the global community. In spite of numerous efforts being taken by global agencies like United Nations, we are yet to arrive at global norms for cyberspace and most importantly global rules for the ethical use of AI. The lead in this can be taken by major AI driven companies who have a global presence and are at the fore front of shaping the AI revolution.

The AI revolution will exponentially reward countries, organisations, industry and individuals who have taken the lead and have become integral stakeholders in this fast emerging ecosystem. India has realised the enormous potential of this technology and has taken several steps to promote AI and its use in all facets ranging from healthcare, education, agriculture and economy. However, it is imperative that the vision gets fully translated into achievable targets on ground and does not remain confined to mere words on papers and reports.

Notes

1. Discussion paper, "National Strategy for Artificial Intelligence #AIFORALL", Niti Aayog, June 2018 at http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf, accessed on April 9, 2019.
2. Statistics at https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/, accessed on April 10, 2019.
3. Technavio blog titled "Top 10 Artificial Intelligence Companies in the world 2018", December 10, 2018 at https://blog.technavio.com/blog/top-10-artificial-intelligence-companies-worldwide, accessed on April 10, 2019.
4. The report makes very interesting reading and can be read at http://www.chilton-computing.org.uk/inf/literature/reports/lighthill_report/p001.htm, accessed on April 15, 2019.
5. Paper submitted by John McCarthy, "History of Lisp", AI lab Stanford University, February 12, 1979 at http://jmc.stanford.edu/articles/lisp/lisp.pdf, accessed on April 18, 2019.
6. Janosh Delcker, "The man who invented the self-driving car (in 1986)" at https://www.politico.eu/article/delf-driving-car-born-1986-ernst-dickmanns-mercedes/, accessed on April 18, 2019.
7. For details of the matches visit https://www.chess.com/article/view/deep-blue-kasparov-chess, accessed on April 22, 2019.
8. For full video of the Google Duplex go to https://www.youtube.com/watch?v=D5VN56jQMWM, accessed on June 21,2019.
9. For accessing the data set go to http://image-net.org/index, accessed on June 21, 2019.

10. Fast.ai is an open source AI learning platform. Blog on training the computer vision agent is available at https://www.fast.ai/2018/08/10/fastai-diu-imagenet/, accessed on June 21, 2019.
11. For details visit https://www.boeing.com/defense/mq25/#/ready-mission, accessed on March 17, 2020.
12. For details go to http://www.riotinto.com/australia/pilbara/mine-of-the-future-9603.aspx, accessed on June 25, 2019.
13. https://www.youtube.com/channel/UCDjRgo5ecEw0Ou78-uJOssg, accessed on June 25, 2019.
14. https://www.bostondynamics.com/, accessed on June 25, 2019.
15. Gloria Philips-Wren, "AI Tools in Decision making Support Systems: A Review", *International Journal of AI Tools,* April 2012 at https://www.researchgate.net/publication/235705583_Ai_Tools_in_Decision_Making_Support_Systems_a_Review, accessed on June 25, 2019.
16. Rasid Abduljabbar, Hussein Dia, Sohani Liyanage and Saeed Asadi Bagloee, "Applications of Artificial Intelligence in Transport: An Overview", *MDPI Open Access Journal* January 2, 2019, from https://www.mdpi.com/2071-1050/11/1/189/pdf, accessed on June 27, 2019.
17. AI market research of Cognilytica Research titled "Data Engineering, preparation and labelling for AI 2019" at https://www.cognilytica.com/2019/03/06/report-data-engineering-preparation-and-labeling-for-ai-2019/, accessed on June 27, 2019.
18. Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women", *Business News,* October 10, 2019 at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G, accessed on June 27, 2019.
19. Note 10.
20. Interview of Marc-Antoine Dilhac, University of Montreal, *UNESCO Courier* 2018-3 at https://en.unesco.org/courier/2018-3/ethical-risks-ai, accessed on July 1, 2019.
21. "Preliminary study on the technical and legal aspects relating to the desirability of a standard-setting instrument on the ethics of artificial intelligence", UNESCO Report 206 EX/42 March 21, 2019 at https://unesdoc.unesco.org/ark:/48223/pf0000367422?posInSet=2&queryId=325cbca9-7ad3-4265-8118-88c3dc451766, accessed on July 1, 2019.
22. Complete code of ethics available at https://www.computer.org/education/code-of-ethics, accessed on June 18, 2019.
23. The Asilomar principles were formulated after the 2017 Asilomar conference of Future of Life Institute. For detailed principles go to https://futureoflife.org/ai-principles/, accessed on July 2, 2019.

24. Greg Allen and Taniel Chan, "AI and National Security", Harvard Kennedy School, BELFAR Centre for Science and International affairs, July 2017 at https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf, accessed on July 14, 2019.

25. Summary of strategy available at https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF, accessed on July 4, 2019.

26. Land Operations, UK Army Doctrine Publication AC 71940 at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/605298/Army_Field_Manual__AFM__A5_Master_ADP_Interactive_Gov_Web.pdf, accessed on July 6, 2019.

27. Daniel Kahneman, *Thinking Fast and Slow*, Farrar Straus & Giroux, 2012.

28. Karel van den Bosch and Adelbert Bronkhorst, "Human-AI Cooperation to Benefit Military Decision Making" at https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-160/MP-IST-160-S3-1.pdf, accessed on July 6, 2019.

29. EMC report titled "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things" at https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm, accessed on July 14, 2019.

30. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation,* Report of the University of Oxford at https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf, accessed on July 8, 2019.

31. Johan Schubert1, Joel Brynielsson, Mattias Nilsson and Peter Svenmarck, "Artificial Intelligence for Decision Support in Command and Control Systems", 23rd International Command and Control Research & Technology Symposium "Multi-Domain C2" at https://www.researchgate.net/publication/330638139_Artificial_Intelligence_for_Decision_Support_in_Command_and_Control_Systems?enrichId=rgreq-5b84363a0705b2e0dda1109c295eb841-XXX&enrichSource=Y292ZXJQYWdlOzMzMDYzODEzOTtBUzo3MTkwMzg0OTc5NTE3NDZAMTU0ODQ0MzU0NTgyMw%3D%3D&el=1_x_2&_esc=publicationCoverPdf, accessed on July 9, 2019.

32. Cuthbertson, Anthony. "Raspberry pi-powered AI beats human pilot in dogfight", *Newsweek*, June 28, 2016 at https://www.newsweek.com/artificial-intelligence-raspberry-pi-pilot-ai-475291, accessed on July 13, 2019.

33. Tamir Eshel, "Russian Military to Test Combat Robots in 2016", *Defence Update*, December 31, 2015 at https://defense-update.com/20151231_russian-combat-robots.html, accessed on July 14, 2019.

34. Thomas McMullan, "How swarming drones will change warfare", *BBC Online News,* March 16, 2019 at https://www.bbc.com/news/technology-47555588, accessed on July 13, 2019.

35. DARPA News, "Gremlins on Track for Demonstration Flights in 2019" at https://www.darpa.mil/news-events/2018-05-09, accessed on July 13, 2019.
36. For details visit https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html, accessed on March 17, 2020.
37. BharatNet Status at http://bbnl.nic.in/BharatNet.pdf, accessed on July 19, 2019.
38. For full policy go to https://data.gov.in/sites/default/files/NDSAP.pdf, accessed on July 23, 2019.
39. https://data.gov.in/ for greater details. Accessed on July 23, 2019.
40. Statistics of UNICEF from https://www.tellmaps.com/uis/rd/#!/tellmap/187250920, accessed on July 23, 2019.
41. Government of India, Ministry of Human Resource Development report of 2016 on "Education Statistics at a Glance" at https://mhrd.gov.in/educational-statistics-glance-2016, accessed on July 23, 2019.
42. Ibid.
43. World Intellectual Property Organisation (WIPO) report "Technology Trends 2019: Artificial Intelligence" at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf, accessed on July 25, 2019.
44. WIPO report, "Global Innovation Index 2019" at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019.pdf, accessed on July 25, 2019.
45. Report by *Analytics India* titled "The Hitchhiker's Guide to Artificial Intelligence 2018-19" at https://www.analyticsindiamag.com/wp-content/uploads/2018/12/The-Hitchhikers-Guide-to-Artificial-Intelligence.pdf, accessed on July 29, 2019.
46. Report of the Artificial Intelligence Task Force at https://dipp.gov.in/whats-new/report-task-force-artificial-intelligence, accessed on July 28, 2019.
47. For constituents of committees at https://meity.gov.in/writereaddata/files/constitution_of_four_committees_on_artificial_intelligence.pdf, accessed on February 8, 2020.

4. Blockchain and Big Data: Enablers of National Security

The blockchain cannot be described just as a revolution. It is a tsunami-like phenomenon, slowly advancing and gradually enveloping everything along its way by the force of its progression.
– William Mougayar

Introduction

It is often said that Artificial Intelligence, blockchain and Big Data analysis would be the three technological pillars on which internet 2.0, the next generation global, smart, intuitive and computing network will rest on. Blockchain is a revolutionary means to verify and attribute information to an entity (could be human or machine) which in spite of having the entire information available for everyone to see in the open domain retains user identity, security and privacy and is immune to manipulation and large scale cyber-attacks. Big data on the other hand provides us the tools to access, organise and analyse large quantities of disparate and unstructured data in various formats in order to provide greater and new insights, as well as helps us in organising data into formats which can be subsequently used by other applications like AI, etc.

The discovery of blockchain is still shrouded in mystery and revolves around the enigmatic personality known as *Satoshi Nakamoto*. No one knows whether Satoshi, the inventor of blockchain technology and the famous Bitcoin is male/female or a group of individuals or organisations using a pseudonym. It all started when the domain name bitcoin.org was registered in August 2008 and in October 2008 Satoshi Nakamoto posted a white paper online on "Bitcoin: A Peer to Peer Electronic Cash System"[1] wherein he(?) introduced a novel method of transferring electronic currency from peer to peer without the mediation of a trusted third party (financial institution) and still being able to solve the double spend problem (The problem of a fraudster utilising the same digital currency for more than one valid transaction, i.e. if a fraudster has got Rs 10 in digital currency and he makes two successful transactions of Rs 10 each in order to fool the digital currency eco-system).

The Bitcoin source code known as Bitcoin core was released by Satoshi in January 2009 under MIT open source licence and is easily available for download.[2] The latest version is 0.18.1 and is 210 GB of data with additional 5-10 GB being added every month. The first Bitcoin transaction took place in 2010 when programmer Laszlo Hanyecz spent 10,000 BTC (Bitcoin) to buy two Papa John pizzas. The cost of one BTC is currently around Rs 8 lakh.

One thing to be taken note of is that blockchain is not only Bitcoin, but something much more useful and larger. Blockchain is an entire ecosystem wherein it is possible to have a fully attributable, secure, immutable and truly distributable open ledger system, where each transaction is entered using cryptographic trust between the entities of the ecosystem and which once made cannot be changed or altered. Because it is open and distributed, all members of the ecosystem can see the transactions but not manipulate them (like a 'read only' word file). The distribution over the entire ecosystem (which can be the global internet) ensures that the system is almost immune from a debilitating cyber-attack. Since, no third party is involved in the transactions, the chances of failure or manipulation due to the third party are completely nullified.

Bitcoin ushered in a wave of crypto currencies, all using the blockchain distributed ledger system. Some of the common crypto currencies are Bitcoin (BTC), Bitcoin cash (BCH), Bitcoin Satoshi Vision (BSV), Ethereum (ETH), Litecoin (LTC), Dash (DASH), Monero (XMR) and ZCash (ZEC). These currencies are traded round the clock on global platforms like coindesk (https://www.

coindesk.com/) and currency valuations keep on fluctuating like any currency exchange.

Satoshi mined the genesis block (block 0) of bitcoin on January 3, 2009 and was rewarded by 50 bitcoins. He suddenly disappeared from the cyberspace in 2011 with his last email to Gavin Anderson, a computer programmer on April 23, 2011. By this time, Satoshi had mined over a million bitcoins. Post disappearance of Satoshi, Gavin Anderson became the lead developer at Bitcoin Foundation. The price of a single bitcoin was virtually nothing between January 2009 to March 2010, when its price was pegged equivalent to $0.003. Currently, the price of one bitcoin is averaging above $11,000. More than 17 million bitcoins out of the total 21 million bitcoins to be mined till 2140 AD have been mined so far. Roughly 1800 new bitcoins are mined every day with one block being added every 10 minutes.

From 2000 onwards, the world has been on a rapid journey towards increasing digitisation and interconnection. This coupled with rapidly falling costs of smartphones, computers, tablets and other computing devices with higher bandwidths, has resulted in a deluge of digital data often termed Big Data which requires special tools to manage and classify. Big Data is generally characterised by three Vs – *volume*, *velocity* and *variety*. *Volume* refers to data sizes ranging from terra bytes to zeta bytes. *Velocity* implies fast refresh rates, which make it extremely difficult to classify and analyse the data entering the system at high speed. *Variety* refers to data from different sources and formats. It could be structured (like access tables), semi-structured (like xml files) or unstructured (like audio recordings, videos, images, text, etc.). Different formats imply logs, text, audio, image and video formats.

According to Gartner, a leading ICT research and consultation company, "Big data is high-volume, high-velocity and/or high variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation".[3]

Storing, classifying, managing and analysing big data is extremely important in the global digital world of today. First, in the digital economy, data is an artificial resource which can be greatly monetised and therefore needs to be protected and utilised. Second, the current AI based technology requires vast quantities of clean and annotated data for learning and testing purposes. Third, analysis of Big Data reveals a number of patterns and "unknown unknowns" which help in optimisation and pattern recognition. Fourth, misuse of big data can violate individual privacy and could lead to manipulation and targeted misinformation campaigns. And lastly, with the coming of Internet of Things (IoT), there will be an exponential rise in the volume, velocity and variety of data being generated and we need to be ready with the necessary tools to properly classify, manage and analyse this vast quantity of data.

This chapter will endeavour to provide a bird's eye view of the disruptive technologies of blockchain and Big Data, their use in industry and defence as well as their impact on the Indian digital ecosystem, economy and other critical sectors from a national security perspective.

Blockchain Technology

Introduction to Blockchain:[4] In the era of fake news and altered reality, blockchain as a technology has the potential to verify each and every piece of information flowing through the cyberspace across geographical boundaries without any third party requirements. This disruptive capability of blockchain has the potential to transform the way items are shipped, Intellectual Property is shared, contracts are written, diamonds and precious stones are mined, organs are donated and even personal images, messages and videos are shared and spread. The misconception among the vast majority of people that "Blockchain is Bitcoin" needs to go. Blockchain as a technology can be broken down into three large groups depending on their usage or application. The first group is digital or crypto-currency. The second group is contracts, and the third group is, other applications.

To understand the underlying concept of blockchain we will look at the way Bitcoin (the reason for creating blockchain technology) works. The underlying concepts used for verifying and adding new transactions as well as generating revenue for the miner, can be carried forward and applied to a host of products and services, as is being done the world over.

Blockchain technology can be understood better in terms of a three layered structure. The bottom most layer is the actual blockchain layer which is part of the Application layer of an OSI or TCP-IP model. The blockchain layer can be compared to a global spreadsheet containing details of all the transactions which have been added right from the start of the spreadsheet (called block 0 or the genesis block). It is a common ledger of all transactions which have taken place and is owned by no one, viewed by everyone, updated and verified by miners (who are awarded reward/remuneration for their work). The middle layer above the blockchain layer is the protocol layer which is used by the client for interacting with the blockchain layer(for adding, transferring or withdrawing crypto-currency). The top most layer is the currency layer or the client/ user interface which provides a simple, easy to use digital wallet to the user/client for managing his crypto currency/currencies. Each currency can have its own blockchain layer like Bitcoin or multiple currencies can share the same blockchain like Counterparty (XCP), which is a crypto-currency that uses the bitcoin blockchain for maintaining its record of transactions.

How to solve the double spend problem and the Byzantine generals problem (Having multiple generals in the battle field who do not trust each other but need some sort of a coordination and communication interface amongst themselves), without trusted third party assistance, had been baffling the digital ecosystem community for years, until the discovery of blockchain system.

In a digital currency ecosystem there are multiple stakeholders: the user, software developers; miners; crypto currency exchanges; merchant processing companies; and crypto wallet providers. In order to enter the crypto currency ecosystem, apart from an internet connection, the user needs to have a unique public key address (similar to a unique email ID), the private key associated with the public key address and the wallet software loaded on the computer or smartphone. The public key address is required so that others can transfer bitcoin (for the sake of simplicity, term bitcoin has been used to denote different crypto currencies) to you, while the private key is required for you to transfer bitcoins from your account to other accounts.

To start transacting in the digital currency ecosystem, the user has to undertake the following steps:

Step 1: Download the digital wallet on to computer or smartphone from app store or various sites like Blockchain.info, Mycelium, Coinbase, etc.

Step 2: After setup, the bitcoin address as well as private key is automatically generated. The bitcoin address is an alphanumeric string of 26 to 34 characters, while the private key is a 256 bit number which in Hexadecimal format (0-9 and A to F) and can be represented in 64 characters. The safety of the private key, is of utmost importance because without its knowledge no bitcoin can ever be transferred from one wallet to another.

Step 3: Bitcoins can be purchased from a crypto exchange wherein payment using a variety of means like credit card/debit card/wire transfers are accepted and corresponding bitcoins are transferred to your wallet, after deducting the transaction fees by the exchange. Unlike regular currencies, a bitcoin can be divided into 8 decimal points with the smallest unit (0.00000001 BTC) being called one *satoshi.*

Step 4: In order to transfer bitcoins, a user requires the recipient's wallet address as well as the private key of his own wallet from which bitcoins are to be transferred. The sender submits a transaction request by entering the details of bitcoins to be transferred from the sender's wallet to the recipient's address and the same is authorised by inputting the private key of the wallet. In case, there is a mismatch in the private key, the transaction is cancelled. Once the transaction is validated a message is broadcast to the network giving the details of the bitcoins which have been transferred from one wallet to another. The recipient immediately receives a notification about the transfer of bitcoins which is unconfirmed. After about ten minutes, the transaction is entered into the new block by a miner and the transaction gets confirmed.

Behind the Scene Activities: Before understanding the complexity behind the working of bitcoin system, it is essential that certain key terms be defined. These are:

- **Blockchain:** A digital open ledger system where records of transactions are kept on multiple computers (*Nodes*) connected to each other in a peer to peer configuration. A number of transactions are clubbed together to form a block and blocks are timestamped and sequentially linked with each other from block number zero (called genesis block) till the latest verified and added block to form the blockchain. Thus, *blockchain is a chain of blocks*.
- **Block:** A block can be considered as a page of a ledger book which keeps account of multiple transactions. Like each page of a ledger book is sequentially numbered, similarly block*s* are also sequentially connected from one block to another. The block*s* are timestamped to identify the sequence of occurrence of blocks. It is the task of miners to add new blocks to the existing blockchain.
- **Node:** These are powerful computers that store and run the bitcoin software. The *nodes* are the heart of a blockchain eco-system. Each node is connected to multiple nodes which continuously exchange information with each other. The blockchain is stored in nodes and the nodes are responsible for verifying transactions, creating new blocks, adding new blocks and sharing information about the blockchain with each other. A *Full Node* contains the entire copy of blockchain data and *Master Nodes* are certain specified *Nodes* that perform other management functions in addition to *Full Nodes*. Anyone can participate to become a *Full Node* however, a *Master Node* is required to keep a large amount of crypto currency as collateral to ensure that agreed rules and protocols are not violated.
- **Miners:** These are a special type of nodes which create and add new blocks to the blockchain. A total of 21 million bitcoins will ever exist in the system. These bitcoin*s* do not exist as of now and a certain number of bitcoins are given as a reward to a *miner* who is the first to successfully solve a computational puzzle (called proof of work) and thereafter is allowed to add a new block to the existing blockchain. Anyone can become a *miner* and more the number of *miners*, the better it is for the

entire bitcoin ecosystem. Since, to earn the reward, a *miner* has to solve a proof of work first, it follows that a *miner node* has to invest a lot on computational processing power and electricity in order to regularly add blocks to the blockchain eco-system. This in turn improves the efficiency and security of the eco-system. The degree of difficulty of solving the proof of work is calibrated such that it roughly takes 10 minutes to add a new block to the blockchain. Nodes verify the proof of work carried out by the *miner* and accept the new block added by the winning miner. This blockchain with the newly added *block* is updated amongst all the nodes and transactions verified while in the meantime *miners* get busy in creating new *blocks* and competing with each other to be the first in working out proof of work. The reward of mining and adding a new block is currently 12.5 bitcoins but, the reward keeps on getting reduced by half after every four years or so (The next change in reward will occur sometimes in 2020-21).

- **Hash Function:** Kindly refer to "Application layer security standards/protocols" under "Security and cryptography" in Appendix A.
- **Proof of Work:** As explained earlier, this is the puzzle each miner has to solve to compete with other miners in order to add a new block to the blockchain. Bitcoin uses the *Hashcash*[5] proof of work system to select the winner *miner*. The bitcoin proof of work is as under:

To find an integer (called a nonce which is concatenation of "number once used") between 0 and 4,294,967,296 which when combined with the data in the new block (which is waiting to be added to the blockchain) and passed through a Hash function will produce a resultant hash that has to start with a pre decided number of zeros.

Finding the given integer (or proof of work) is purely a function of luck and computational power.

The step by step procedure for adding a new block to the *blockchain* is as under:

Step 1: Sender (client of a particular crypto wallet) inputs the quantity of bitcoins required to be transferred to the recipient's address (public key) and signs off the transaction using his private key. The Wallet provider verifies the transaction by running a small programme which confirms that the transaction has been signed by a valid private key (confirmation is calculated without knowing the private key of the sender).

Step 2: The wallet provider then transmits the transaction into the blockchain network where it is kept in a pool of unconfirmed transactions, waiting to be picked up by a miner for confirming it and adding it to the latest block.

Step 3: Bitcoin miners pick up transactions from the "pool of unconfirmed transactions" and bunch them into a block. Transactions are picked up such that the total block size cannot exceed 1 MB and transactions offering higher processing fees are picked up before other transactions. The miners thereafter verify each transaction by looking up the entire blockchain and ensuring that the sender has the required or more number of bitcoins available in his wallet than the quantity he is transferring. Each miner is at complete liberty to select the unconfirmed transactions which they want to add to their block. Also, two miners can have the same unconfirmed transactions in a block.

Step 4: Miners thereafter compete with each other to solve the proof of work problem as applicable to their chosen block. This exercise is very intensive in computational resource and requires a lot of electricity and CPU power as finding the *nonce* requires a brute force approach.

Step 5: The miner who solves the proof of work first broadcasts the same along with the block to all the other miners for verification.

Step 6: The other miners will verify the fastest submitted proof of work by hashing the nonce with the block and if found correct will add the block to the blockchain. This new added blockchain is then spread to all the nodes.

Step 7: After a block is added in the blockchain then each additional block that is added after that block, is counted as a confirmation of that block. For example if the block containing a given transaction is block No. 102 in the blockchain and presently the blockchain is till block No. 106, then it is said that the transaction of block 102 has four confirmations. The more confirmations a particular block gets, the more difficult it is to alter and hack the contents of the blockchain. After a new block is added to the blockchain, the miners get busy adding new blocks after solving the proof of work puzzle.

Advantages and Limitations of Crypto Currencies: Crypto currencies like Bitcoin have created a paradigm shift in the manner in which currencies are transacted and used globally. It is therefore important that a holistic view is taken, on both the merits as well as limitations, of such currencies prior to arriving at any particular view point.

Advantages of Crypto Currencies

- **Transparency and Use of Open Source Algorithm:** Each crypto currency transaction is fully transparent and visible to all. The programmes used for running the currency are open source and available for everyone to analyse and make improvements. In the era of backdoors in proprietary software, crypto currencies like bitcoins are open and transparent.
- **Immunity to Cyber Attacks:** Because crypto currencies work on a peer to peer network which is spread globally and is mined and confirmed by hundreds of nodes, it is nearly impossible to bring down the complete ecosystem or cripple it by a massive cyber attack. Having multiple copies of the blockchain spread across multiple geographical locations under different jurisdictional territories adds to the strength of the system. A node, even if brought down by a cyber attack can start afresh and can copy the latest blockchain from other nodes.
- **No Boundaries:** The digital crypto currency is spread across the globe making transfer of funds between multi parties across geographical boundaries extremely easy and convenient.
- **Personal Data Privacy/Relative Anonymity:** Opening a crypto currency wallet does not require any major personal information to be given to the wallet provider. This ensures that the privacy of

digital wallet holder is preserved even when the wallet provider data base is hacked or accessed. Also, transferring funds from the wallet requires the private key, which is exclusively held by the digital wallet holder.

- **Lower Transaction Fees:** On an average, Bitcoin transaction fees are less than a per cent of the transacting amount whereas credit card transaction fees generally range from 3 to 5 per cent.
- **Faster Settlements:** Bitcoin settlements are completed in 10 minutes on average. Credit card settlements, especially between different countries generally take three days.
- **Inflation Proof:** A total of 21 million bitcoins can exist in total. By the current rate of generation of blocks (roughly 10 minutes) and the block reward to miners getting halved every four years or so, all bitcoins will be mined by 2140. Since Bitcoins are not directly dependent on any single currency or commodity, they are relatively inflation proof. However, since digital currency functions in a more or less unregulated ecosystem, it is susceptible to wild fluctuations.
- **Immutable Transactions:** Once the transactions are entered on the *blockchain* they are considered immutable, especially when a particular block has five or more confirmations.
- **Ease of Operations:** Opening a wallet and transacting using crypto currency is very easy and hassle free.
- **No Third party Regulation:** Crypto currency works on a peer to peer system with user free to choose from multiple exchanges and wallet providers.

Limitations of Crypto currencies

- **Loss/Compromise of Private Keys:** If a user loses his/her private key, then there is no way to retrieve the crypto currencies associated with that particular address. In December 2018, Gerald Cotton, CEO of Canadian crypto exchange Quadriga CX died in Jaipur and was reportedly the only holder of the exchange's private key which was a major hurdle to overcome.
- **Lack of fool proof anonymity:** At the first instance, it seems that digital currency offers complete anonymity. However, recent

advances in statistical techniques and pattern recognition can successfully profile upto 60 per cent of digital crypto currency user like Bitcoin. Since all the transactions that have taken place are visible to everyone and are linked to public addresses of user, digital currencies are pseudo anonymous and not anonymous. Japan's National Police Agency (NPA) is planning to launch a new software that will keep track of all crypto currency transactions within the country.[6]

- **Scams and Frauds:** Like other internet applications, digital currency users are also susceptible to social engineered scams and frauds, especially when they are lured into sharing their private keys with other parties.
- **Lack of Trust by different Cross Sections of Society:** Crypto currencies are generally well accepted by the youth and technical savvy population. However, elderly people especially women find it difficult to trust crypto currencies which is a major barrier to cross.
- **Large Element of Volatility:** Since crypto currencies are un-regulated and not linked to any other currency or commodity as well as traded across the globe 24x7, they tend to demonstrate wide volatility which can greatly increase the risk of possessing these currencies in the short term.
- **Used for Illegal Activities:** The crypto currencies offer many advantages to criminals because of their pseudo-anonymous nature, lack of regulation, global presence and ease of operation. This has been exploited by the criminals and crypto currencies especially Bitcoins have been extensively used for money laundering, illicit drug transactions and terror financing.[7]
- **Illegal to Possess and Trade in Certain Countries:** Certain countries like Algeria, Bolivia, Morocco, Nepal, Pakistan and Vietnam have banned any and all activities of crypto currencies.[8] Thus, citizens of these countries will be violating law in case they possess or trade in crypto currencies.

Major countries Stand on Crypto Currencies:[9] A large number of countries have accepted crypto currencies while some have out rightly banned them and others are fence sitters and have yet to fully qualify their stand on such currencies. Irrespective of a country's stand, almost all countries have issued a number of advisories to their citizens about the pitfalls of such type of radical currencies. The pitfalls are: the crypto currencies are not issued or guaranteed by any state; the added risk due to high volatility; the global sector of running exchanges and mining currencies is unregulated, so there is a personal risk for individuals and organisations who deal with crypto currencies without any legal recourse. Moreover there is widespread use of these currencies for illegal activities.

Countries like Canada, Australia and Isle of Man have recently amended their money laundering and counter terrorism laws to include crypto currencies and have mandated banks and other institutions dealing with crypto currencies to fulfil all legal obligations prior to carrying out any transactions of crypto currencies. Some countries like Qatar and Bahrain do not permit their citizens to transact in crypto currencies within their territorial jurisdiction, but have no restrictions in case such transactions were carried out abroad.

Countries like Bangladesh, Iran, Thailand, Lithuania, Lesotho, China and Columbia permit their citizens to transact using crypto currencies, but have banned financial institutions from doing so within their territorial jurisdiction.

The Reserve Bank of India (RBI) vide its press release dated April 2018 has stated the following:[10]

Reserve Bank has repeatedly cautioned users, holders and traders of virtual currencies, including Bitcoins, regarding various risks associated in dealing with such virtual currencies. In view of the associated risks, it has been decided that, with immediate effect, entities regulated by RBI shall not deal with or provide services to any individual or business entities dealing with or settling VCs.

Though there is no particular ban on trading in crypto currencies by individuals, it has become next to impossible to trade in these currencies from India. This is because by banning entities regulated by RBI from dealing with crypto currencies, the establishing of crypto exchanges in India and trading in crypto currency using

Indian fiat currency (Rupee) is illegal. In March 2020, the Supreme Court of India in the case of Internet and Mobile Association of India V. RBI has quashed the RBI circular of April 2018 and has effectively allowed trading in crypto currencies within India. The RBI is contemplating of launching its own digital currency called *Lakshmi.*[11] Facebook is also planning to launch its own crypto currency called *Libra.*[12]

Blockchain based Smart Contracts: A contract can be defined as an agreement carried out between two or more parties to carry out/ not carry out any action in exchange for a mutually agreed remuneration. One of the major problems in contract execution is the development of trust amongst the various parties to the contract which at times results in legal recourse, time delays and commitment of additional resources.

A smart contract, on the other hand ensures trust through the code. In simple terms, it implies that remuneration is automatic as soon as the conditions of the contract are fulfilled. In fact, the role of parties to the contract is over the moment the contract is enforced and made to execute automatically as per code. Thus trust is defined and executed by the code automatically without any discretion.

A smart contract is defined by three major characteristics. First, autonomy. This implies that once a smart contract has been initiated, it requires no further inputs and will confirm the successful completion of conditions by various parties and transfer requisite remunerations on its own, without any other external input. Second, self-sufficiency. This implies that all necessary resources required to check the successful completion of various conditions of the contract as well as disburse remuneration are inbuilt with necessary authorisations in place. Third, decentralisation. This implies that the smart contract is available on multiple nodes as part of a strong blockchain so that its execution is more or less guaranteed. The smart contract has to execute the pre specified code. The code itself is tamper-proof as it has been in built into a crypto enabled block on the blockchain.

A vending machine is an example of a smart contract. The machine accepts money as input and the moment right amount is inputted to the machine, it dispenses out the corresponding item. Another example of a smart contract could be the automatic distribution of inheritance amongst beneficiaries post death of a person or gifting a person on her birthday.

Having only one type of contracts might not be the right way to progress in the future and it is important that the society, organisations and governments of the day, choose those contracts which could be either technically binding code contracts or legally binding human contracts.

The smart contract ecosystem is presently yet to fully mature and is susceptible to hacks and compromise. The most famous one was the Distributed Autonomous Organisation (DAO) hack of 2016. The DAO was a virtual venture capital fund developed by a block chain company (slock.it) and operated on the Ethereum blockchain platform. The DAO went live on April 30, 2016.

As part of the virtual venture capital fund, anyone could become an investor in the DAO, by purchasing tokens in lieu of Ether (crypto currency of Ethereum). The Ethers collected from the investors were pooled to constitute the corpus of the venture capital fund. Thereafter, any token holder could become a contractor and submit a proposal for project funding using the pooled corpus. The various proposals were thereafter voted on by the token holders (investors). If a proposal was voted for by 20 per cent or more of the total tokens, then the funds would be automatically transferred to the contractor's account and the smart contract submitted by the contractor executed. The returns (Ether) generated by the proposal would be automatically transferred to the participating investors as reward.

The initial offer of DAO was opened to the public in May 2016 wherein 100 DAO tokens were offered in exchange for one Ether. A total of 12.7 million Ethers (equivalent to $150 million at that time) were raised as part of the initial offering. On June 16, 2016, the DAO got hacked when an attacker was able to exploit a "recursive call exploit" vulnerability of the code and was able to siphon off 3.6 million Ethers. However, there was an inbuilt time period of up to 27 days before the Ethers would be finally transferred into the attacker's account. This gave the Etherium community the time to execute a hard fork of their blockchain on June 20, 2016 and the entire siphoned off Ether was eventually returned to all the legitimate investors.[13]

An Overview of Ethereum: Turing complete Virtual Machine: In his seminal white paper Satoshi Nakamoto, envisaged not only the blockchain platform (distributed ledger system) and Bitcoin protocols but also wrote about *Turing completeness,* or in other words the ability of a single universal platform to run any coin, protocol or blockchain. In order to expand the scope and utility of blockchain based systems to handle complex tasks such as smart contracts, a Turing Complete platform is required, which is what Ethereum is all about.

Ethereum is a platform and programming language for building and publishing distributed applications. It is a complete ecosystem capable of running any distributed application and protocol. The concept of Ethereum was envisaged by Vitalik Buterin in a white paper released in November 2013.[14] Rather than running a single kind of operation like Bitcoin, Ethereum offers the user the capability to develop and run any type of distributed application within the Ethereum ecosystem. It uses two types of currencies. First, Ether which is similar to Bitcoin and is awarded to miners who successfully add blocks to the Ethereum block chain. Second, gas which is given as a transaction fee to miners to run the smart contracts and is dependent on the number of computational cycles required for executing the contract.

In Ethereum, a user is allocated an account and transactions take place between accounts. Each account consists of four fields. First, *nonce* which acts as a counter to ensure that each transaction is processed only once. Second, current Ether balance of the account. Third, *Contract Code* and lastly, link to account's storage space. There are two types of accounts. The first is the *Externally owned account*. These accounts do not have any contract code and are operated by using the private key of user. These accounts are capable of sending messages to other accounts in the Ethereum ecosystem by creating and signing transactions. The second type of accounts are

Contract accounts. These accounts are used to run the contract code. The contract accounts get activated by receiving a message and these messages allow the contract accounts to read/write into the internal storage space of the account, execute code of smart contract, send messages to other accounts or create new contracts.

The transaction which is used for sending a message from an account consists of six fields. First, recipient of the message. Second, signatures identifying the sender. Third, amount of Ether to be transferred from sender to recipient. Fourth, an optional data field. Fifth, STARTGAS value which lays down the maximum computational steps the transaction is permitted to execute and lastly, GASPRICE which is the fee that the sender is willing to pay per computational step. The STARTGAS and GASPRICE are unique features of the Ethereum ecosystem and ensure that hackers are unable to execute infinite loops inside the transaction.

The code in Ethereum is written in byte sized low level language and is called the *Ethereum Virtual Machine (EVM)* code. Each byte executes one operation.

There are three major types of applications which can run on the Ethereum ecosystem. The first are financial applications and these not only include crypto currencies but an entire bouquet of financial goods and services like sub currencies, derivatives, commodities, hedge fund controlling, saving wallets, wills execution, etc. The second types of applications are semifinancial which include automatic payment of remuneration after an agreed task has been completed, like pay outs to winners of a tournament, tokenised contracts and partial ownership of assets, etc. The last type of applications are non-financial and include activities like online voting, tracking of shipping parcels at various stages, health care data management and tracking, intellectual property and patent protection, etc.

Use of blockchain in National Security: The key characteristics of the blockchain ecosystem like distributed ledger, sequential timestamp bound tracking of changes, extremely high resilience to network disruptions and cyber-attacks and immutability of records once confirmed in the blockchain, make the system ideal for implementation in government and national security structures.

The first major use of blockchain technology is for managing data integrity. In today's world of deep fake, it is extremely important to trust any digital content (could be video, audio, logs, GPS fixes, documents, etc.) as it moves from one end of the network to another. The blockchain ecosystem is the most ideal candidate to verify the contents and the originator of digital information, as it is exchanged between various users. Apart from this, the information once encoded into a block cannot be altered or wished away, even after the destruction of a number of nodes running the blockchain ecosystem. This time stamped irrefutable flow of information between different users is critical for complex and time critical operations of the defence forces.

The second major use of blockchain technology is for managing the supply chain integrity of complex systems and platforms. The present generation of systems and platforms are extremely complex machines whose parts and applications are sourced from around the globe. There is always a doubt that an adversary could place a hidden backdoor, either in the hardware or software, which could make the system extremely vulnerable and prone to error and destruction at critical moments. On October 4, 2018, *Bloomberg* reported that China had inserted a tiny backdoor chip into the motherboards that were shipped to around 30 US companies including Apple and Amazon.[15] Ensuring supply chain integrity is also crucial while transporting sensitive minerals, materials, systems and equipment from one place to another. Blockchain technology ensures that each chip, component and code of software inserted at any stage in the procurement and assembly cycle around the globe, can be traced back to the originator and can be compared and verified with the original blueprints, software, components, as well as assembly vendors and workers.

Another major use of blockchain technology in national security and government is, its use in executing smart contracts to ensure transparency and weed out corruption. This would ensure that payments to various contractors and welfare beneficiaries are automatically transferred on achieving required milestones in the project execution phase.

Due to its extremely resilient and survivability characteristics, blockchain is ideal for providing emergency communications in disaster hit areas. In addition, blockchain based systems can be used to execute smart codes which require no human intervention and are self-executable based on pre designated triggers. These smart codes can be utilised as additional safety mechanism to prevent inadvertent launch of missiles and other such operational and strategic weapon systems.

Indian Blockchain Eco-System and Initiatives: The National Association of Software and Services Companies (NASSCOM) and Avasant India have collaborated and released a comprehensive report on the blockchain ecosystem and its implementation in India in March 2019.[16] Salient aspects of the report are given in the succeeding paragraphs.

The year 2018 has been the global watershed moment for the blockchain industry wherein investments in blockchain based crypto currencies and industry have reached more than $20 billion. The earlier versions of blockchain (Blockchain 1.0 and 2.0) had major limitations in terms of the number of transactions per second, as well as heavy energy consumption which made them unsuitable for large scale implementation. The latest version of Blockchain 3.0 systems which are based on Directed Acyclic Graphs (DAG)[17] have no such limitations and have demonstrated more than 10,000 Transactions per second (TPS). They also use relatively less energy which makes them suitable for implementing enterprise blockchain technology and an ecosystem capable of fast scalability and wide implementation.

Globally, there is an acute shortage of blockchain developers with only 45,000 to 60,000 competent developers available worldwide. This presents India with an enormous opportunity to upskill its STEM workforce in this field and become the blockchain service provider to the world. However, to realise this dream, India has to introduce enabling regulations and policies on priority, to stimulate and invigorate the blockchain ecosystem and encourage new startups in this highly competitive as well as rewarding field.

In India, the initiative to implement blockchain and establish its ecosystem has been taken by the public sector. More than half the state governments in the country have invested in the blockchain industry. The two leading states in this regard are Telangana and Andhra Pradesh. The primary utilisation of blockchain infrastructure by the states has been in land registry, securing digital certificates and farm insurance. Apart from these, blockchain is also being employed in citizen health record management, benefit distribution, identity management, power distribution, duty payment, vehicle lifecycle management, organ tracking for transplant, chit fund operations management, micro financing for self-help groups and cybersecurity. The bulk of the initiatives in the public sector were taken in 2018 and as of March 2019, 92 per cent of the projects are in Proof of Concept (PoC) and Pilot stage while balance 8 per cent projects have gone live.

The Indian blockchain industry has been a laggard in comparison to the other leading global companies in this field. Indian startups in blockchain have been able to attract only 0.2 per cent of the global startup investments in this field. A major reason for this is the absence of well defined policy and regulatory framework for blockchains and crypto currencies. Initially, a major portion of startup funding was geared towards crypto exchanges like Unocoin and Zebpay, which had to disable trading through fiat currency, after the RBI directive.

Europe is the world leader both in the implementation as well laying down policy and regulations on the blockchain technology with more than 50 per cent of global enabling regulations coming from it. In India, blockchain is being mostly used in banking, financial services and insurance (BFSI), health care, retail and logistic sectors.

A total of 26 countries have established Fintech/Blockchain regulatory sandboxes which enable startups and technology providers to test their blockchain products and services in a controlled environment with a limited number of consumers for a trial period, without being subjected to regulations. This enables live beta testing of products and services so that errors and problems noticed during the testing phase are removed prior to the blockchain going live in real world.

India accounts for only two per cent of the global blockchain startups presently. However, a large number of factors like an English speaking STEM educated population, relatively lower rates of services and cheap internet access and electricity tariffs, provide the right mixture for it to become a global powerhouse for providing cheap and reliable Blockchain as a Service (BaaS) solutions. What is lacking are enabling regulations and policies, so that a conducive and growth oriented platform is provided to startup companies, along with necessary assurances to the global investor and client community.

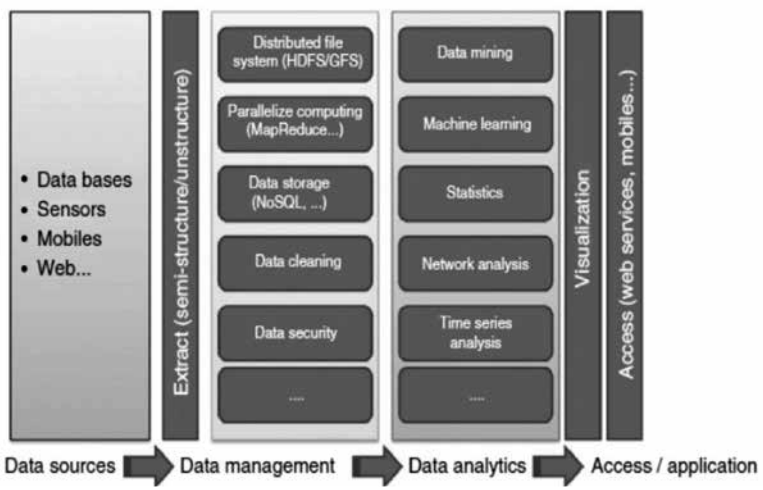
Big Data Technology

Introduction to Big Data:[18] As stated earlier Big Data is characterised by three Vs namely *Volume*, *Velocity* and *Variety*. Recently, two additional Vs have been added to the definition of Big Data – these are *veracity* and *value*. Veracity implies the level of variance in the data residing within the data set, or how closely correlated or spread out the data is. Value implies the benefits and trade-offs afforded by the mining and analysis of the Big Data.

Big Data analytics can be broadly classified under four steps. These are:

- **Data Source:** This implies the identification and extraction of data from databases, sensors, GPS coordinates, health records, mobiles, web, etc.
- **Data Management:** This entails arranging extracted data into easily manageable structures, which facilitates its further analysis. Data can be arranged into Distributed File Systems like Hadoop Distributed File System (HDFS)/Google File System (GFS), structured using applications like MapReduce, cleaned and stored in databases like NoSQL on the cloud or hybrid cloud platforms for easier, faster and smarter access.
- **Data Analytics:** A variety of data analytic tools like data mining, machine learning, statistics, network analysis, etc. are employed on the stored data depending on its type, structure and the associated value which needs to be extracted from it.

- **Data Access/Application:** The visualisation, presentation and dissemination of analysed data in various forms and formats.



Source: researchgate.net

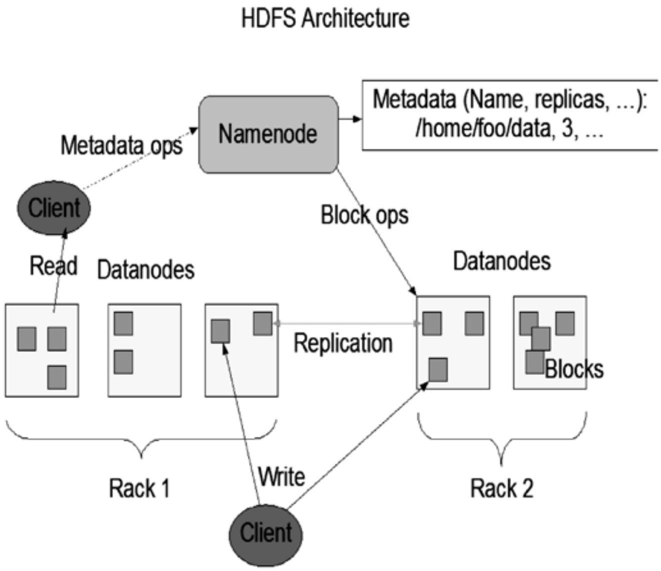
Major Big Data Analysis Platforms: A large number of proprietary and open source Big Data analysis platforms are available in the market. Details of the popular ones are given as under:

- **Google Cloud Platform:** The Google cloud platform offers a simple and server less Big Data analysis service, which can be tailor made as per requirement. The major advantage of the Google cloud platform is its open architecture and easy integration with a variety of open source tools like Apache Spark and Hadoop. A large number of applications like Big Query for analysing large quantity of data ranging from Giga Bytes to Penta Bytes and Cloud Pub to input millions of data points per second into the data set are available, along with different visualisation platforms for easy assimilation and extracting relevant Business Intelligence (BI).
- **Hadoop:** Apache Hadoop is a series of programmable languages which collectively create an ecosystem for storing, managing, analysing and visualising big data. The Hadoop ecosystem consists of four major elements namely HDFS, MapReduce, YARN and Hadoop common.

- **ASTERIX:** It is an open source system for big data management and analysis. The strength of ASTERIX lies in dealing with semi-structured data including its ingestion, storage, management, indexing, retrieval and analysis.

Apache Hadoop Eco-System:[19] The Hadoop ecosystem is an open source resource of multiple software written in *Java* language which has been specifically created for working with big data. It uses commonly available computer hardware and resources and is extremely simple to work with. It can be suitably expanded to meet multiple requirements and is fault tolerant. In essence, the Hadoop ecosystem allows a network of multiple computers to store, process and analyse multiple portions of big data, simultaneously resulting in faster processing and management of big data. The various components of the Apache Hadoop ecosystem are as under:

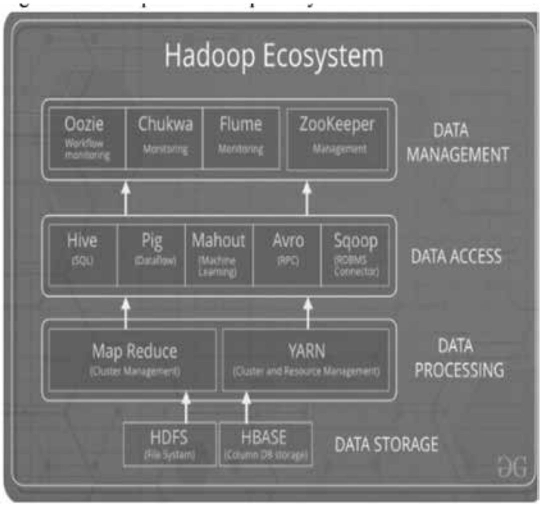
- **HDFS** The big data in Hadoop ecosystem is stored in distributed data storage clusters. A HDFS cluster comprises of a *Name Node* which is used for managing the multiple *Data Nodes* which are used for storing big data. The clients access the Name Node for ascertaining the specific Data Node's location and carryout actual read/write operations on Data Nodes.



Source: Hadoop.apache.org

- **Map Reduce:** The term was initially used by Google's proprietary big data analytical framework but has since been used for denoting the framework of splitting-applying-combining Big Data, for parallel distributed processing, especially in the Hadoop ecosystem. The Map Reduce framework consists of two parts, the *map* which takes its input as Big Data and is used to split it into independent blocks for simultaneous parallel processing; while the *reduce* function takes the output of *map* function as input and further processes the data independently. In the Hadoop ecosystem, the compute and storage nodes are the same. This implies that the Nodes running the map and compute functions and storage of Big Data belong to the same cluster. The Map Reduce framework is responsible for splitting a *job* into multiple *tasks*. To schedule and track the progress of various tasks as they are being processed simultaneously, the Hadoop ecosystem uses *a job tracker* which resides in the Name node and acts as the master controller and multiple *task trackers* which reside in Data Nodes and continuously provide inputs and receive instructions from the *job tracker*. The *job tracker* is responsible for scheduling *tasks*, monitoring *tasks* and re executing failed *tasks*.
- **YARN:** The YARN framework in Hadoop is responsible for managing and tracking resource (cpu, memory, etc.) allocation and management amongst various application*s* running in a cluster of multiple Nodes (or separate computers). It consists of a single global Resource Manager and multiple Application Managers (one manager per *application*. An *application* could be a single *job* or multiple *jobs*) and Node Managers (One manager per Node/computer). The Resource Manager is the final authority on all resource allocations. The Application Managers negotiate resources with the Resource Manager and after approval instructions for allocation of resources per application are given to various Node Managers. Regular monitoring of resources allocation and progress on various applications is carried out by *Resource*, *Node* and *Application* managers and together they constitute the data-computation framework in the Hadoop ecosystem.

- **Hadoop Commons:** These are open source shared utilities and libraries containing a host of applications which can be utilised for storage, management and analysis of big data in the Apache Hadoop ecosystem.



Source: geeksforgeeks.org

Use of Big data in National Security Storing, managing and thereafter analysing big data is a complex technical challenge which requires the best of skill sets and state of art digital infrastructure like massive data centers and high end super computers to overcome. It is therefore obvious that building a big data ecosystem to store and thereafter generate intelligence out of the data is not everybody's cup of tea. Those countries that do not encourage and indigenously build large scale big data ecosystems will be left at the mercy of powerful nations who will not only extract and store their big data but will monetise and use it to fuel further innovations in the knowledge based economy of today.

The world is witnessing a big data explosion. Presently, 2.5 quintillion bytes of data are being generated every day in the world[20] and by 2020, there will be around 40 trillion gigabytes of data (40 zettabytes). In fact, the pace of data generation is so fast that we have created 90 per cent of the world's total digital data in the last two years alone. This is poised to increase exponentially as IoT based devices become extremely cheap and universally available and 5G wireless services replace current wireless mobile services the world over.

The depth and scope of national security challenges facing a nation state have also grown manifold and range from terrorist activities and lone wolf attacks to environmental disasters, financial frauds, money laundering, weapons and drug trafficking, cyber-attacks, cyber-crimes, cyber-espionage, misinformation campaigns and use of dual use technology like drones to hit high value targets. Extracting intelligence out of Big Data in quick time, is emerging as a major force multiplier for overcoming almost all the major national security challenges, being faced by a nation state today.

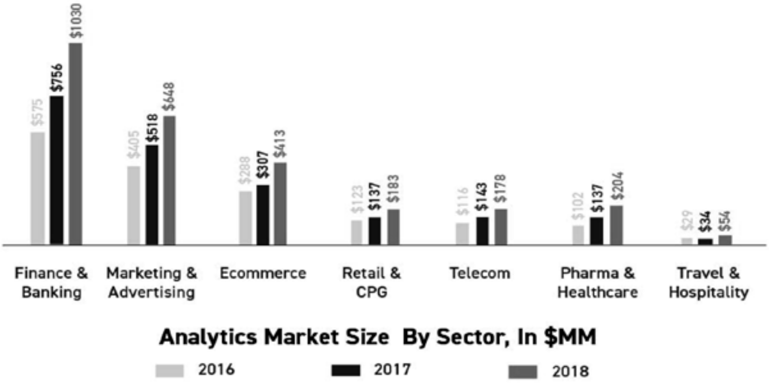
The view in the world community is that data is the new oil. Thus, a comparison between both the commodities is very much in order. First, unlike oil where value resides in each drop, the real value of data resides in Big Data and not, single bytes of data. Second, companies who are able to extract intelligence out of Big Data, generate enormous revenues like major oil giants. Facebook's and Google's primary source of revenue is their Big Data and its associated intelligence. Third, unlike oil which is a natural resource, data can be created indefinitely. Fourth, unlike oil which gets expended once utilised, the same Big Data can be monetised again and again and offer fresh insights and utility each time.

In 2012, only about 0.5 per cent of the total data generated was analysed. In comparison, it is estimated that in 2020 almost 37 per cent of the total data generated would be analysed. The big data analytics market is a $49 billion industry presently which is growing at a CAGR of 11 per cent and is expected to reach $103 billion by 2023.

Indian Big Data ecosystem and Initiatives:[21] Based on a recent study by AnalytixLabs and *Analytics India Magazine* (*AIM*), the current analytics, data science and big data industry in India has an annual revenue of $2.71 billion which is growing at a CGAR of 33.5 per cent. The expected revenue is likely to grow to USD 20 billion by 2025. In comparison, the global big data and analytics market had revenues of $168.8 billion in 2018 and is projected to reach $274.3 billion in 2022 growing at a CGAR of 13.2 per cent.

Of the total revenue generated in 2018, roughly $1.7 billion came from analytics exports to USA alone (roughly 64 per cent of total revenue) and what is more encouraging is that the revenue from USA is growing at a rate of 45 per cent year on year.

The Finance and Banking sector generates the maximum revenue ($1 billion or 38 per cent), followed by marketing and advertisement (24 per cent) and e-commerce (15 per cent). The maximum jump in year on year growth in revenue has been witnessed by the travel and hospitality sector (from $34 to 54 million YoY or 61 per cent) followed by Pharma and healthcare ($137 to 204 million).



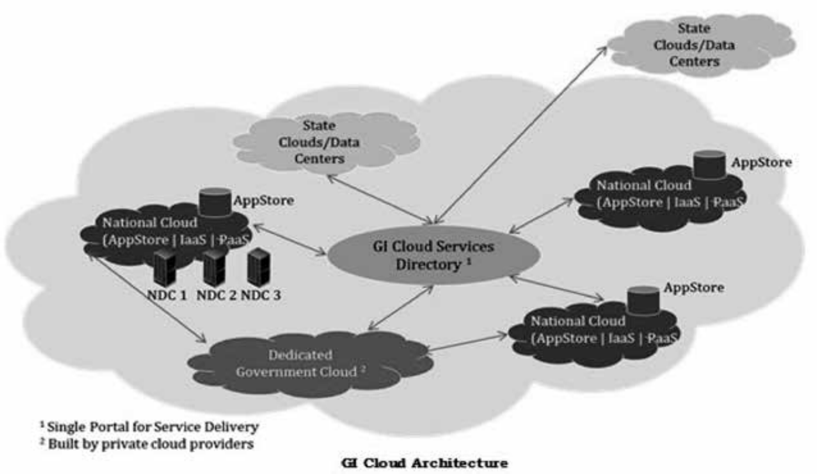
Source: AnalytixLabs & AIM

The Delhi NCR and Bengaluru hubs account for almost 55 per cent of the total revenue (individual share of 28 and 27 per cent respectively). Other major analytics, data science and big data hubs are Mumbai, Hyderabad, Pune, Chennai and Kolkata.

Large companies like TCS, Wipro, Genpact and Tech Mahindra employ up to 40 per cent of the Indian workforce while startups (having an employee base of under 200) employ about 28 per cent of the workforce. Most of the professionals have a master's degree with the ratio between under grad and grad around 2:3.

The government of India has embarked on an ambitious project of providing cloud based e-services nationwide through a

"GI Cloud" based cloud computing ecosystem called "*Meghraj*".[22] The various components of *Meghraj* include state and national clouds, e-Governance App Store, *Meghraj* service directory, cloud management office, cloud auditors and cloud service providers.


State Clouds/Data Centers
State Clouds/Data Centers
AppStore
National Cloud (AppStore | IaaS | PaaS
AppStore
National Cloud (AppStore | IaaS | PaaS
GI Cloud Services Directory 1
NDC 1 NDC 2 NDC 3
AppStore
National Cloud (AppStore | IaaS | PaaS
Dedicated Government Cloud 2
1 Single Portal for Service Delivery
2 Built by private cloud providers
GI Cloud Architecture

Source: MeitY

The national cloud was launched by National Information Centre (NIC) in February 2014 (https://cloud.gov.in/) and offers Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS) to various organisations, businesses and even individuals. The Government App Store (http://apps.nic.in/) was launched in May 2013 and hosts 61 applications across 26 sectors.

Conclusion

The world is witnessing exponential growth in digital connectivity, data access speeds, internet connected devices, processing power, storage and battery performances. The above has been made possible due to rapid advancements in ICT technologies. These range from high speed wireless networks like 5G, cloud computing and storage, cheap availability of IoT devices, e commerce, banking and financial platforms, rise of global social media and innovation companies, widespread use of ICT based service aggregators like taxi, health care and other services and major breakthroughs in AI, Big Data analysis, blockchain, nano technology, storing and computing resources and power pack solutions.

As the rate and quantity of data generation rises exponentially, the need for storing, processing and analysing this huge artificial resource will rise. The technology based economy of the world will thereafter be carved up into two halves. First, the states and global corporations which have the tools and structures to manage, create and derive intelligence and revenue from this vast unending pool of data; and second, the states and corporations who will be dependent on the first half, to manage store and utilise the data which has been generated by indigenous users and connected devices. Thus, the concept of data sovereignty or the right to manage, store, analyse, derive intelligence and monetise own generated data will begin to take centre stage in global discussions on strategy, economics and geo-politics.

In the era of cyber-attacks, misinformation campaigns, deep fakes, digital anonymity and non-attributability, blockchain provides a reliable, secure, distributed, trusted and open system with an extremely resilient structure, to withstand debilitating cyber-attacks. Though the technology is sometimes erroneously equated with digital or crypto currency alone, it is a complete ecosystem capable of much more than being just used for generating and processing Bitcoin or other crypto currencies. Use of Blockchain for executing smart contracts, maintaining land and other records, employment in financial and banking sector and distribution of e-services has seen a rapid rise since 2102 and has been found to be a transparent, scalable and easily implementable solution. The previous drawbacks of the system, ranging from long delays in adding blocks and scalability, have been fixed in the later versions. The availability of various blockchain ecosystems including Ethereum on open source platforms, increases the systems appeal and acceptance. A large number of Indian central and state governments have found merit in the blockchain ecosystem and have developed a number of running and pilot use cases. However, more needs to be done and much faster.

Storing, managing and analysing Big Data is a strategic challenge which is bound to arise as states assert the notion of data sovereignty and accept citizen digital privacy as a fundamental right, with the state being responsible for it being assured. Storing, management and analysis of Big Data is an extremely complex technical challenge with capabilities restricted to a few multinational companies and countries. This provides an incredible leverage and creates a sharp divide between the haves and have nots. Let us consider the hypothetical example of a state desirous of implementing data localisation in its territory, but which finds it impossible to do so due to refusal of outside multinational companies and unavailability of indigenous technology and industry. It could also happen that the content of Big Data is such that a state would not like any outside company to handle and analyse it.

In the technology driven world of today a state of the art, cheap, secure and clean cyber infrastructure is a major strategic asset and leverage. The major components of this infrastructure include: pan India high speed, high bandwidth OFC core based backbone with 5G based wireless interface. There is a need of multiple high capacity data centres and cloud storage platforms with high speed super computers for parallel and distributed processing. Another important component of the big data ecosystem is having high tech industry capable of creating components, devices, processes and applications dealing with Big Data storage, computation, analytics and dissemination. Also, skilling and retaining a suitable workforce with high end skill sets and providing commensurate incentives and opportunities for growth and progress for them, is another extremely important part of the Big Data ecosystem. A culture of high end research and development with emphasis on breakthrough technology and patent filing, needs to permeate throughout specially created high tech clusters, which develop and build up a global reputation of providing high end solutions, at extremely competitive rates.

The role of government, academic institutions, R&D organisations and ICT industry cannot be over emphasised. Developing a high end niche cyber infrastructure and ecosystem capable of competing across the globe, requires a whole of nation approach. As brought out earlier, cyberspace is an intensely competitive and fast evolving domain where the winner takes all. India, due to its large STEM workforce coupled with a knowledge of the English language and computer coding skills, has the potential to become a global leader in providing smart and competitive solutions in the high end fields of AI, blockchain and Big Data. These technologies are bound to replace a large number of traditional jobs and would give rise to a whole new range of previously unknown streams of job and wealth creation. The country which is at the fore front of these technologies would be able in an advantage to grab and exploit these opportunities.

It is therefore important that the government acts smart and acts fast. The role of the government is to lay down and execute policies and frame works that fast tracks creation of high end cyber infrastructure, R&D organisations and industry with suitable high skilled work force. Towards this end, creation of special economic zones and clusters, providing cheap and high end digital infrastructure and electricity, promulgating industry and start up friendly laws and policies, improving ease of doing business and providing tax breaks and customs exemptions comparable with the best in the world are some of the important steps which the government needs to take. Education institutions and R&D organisations need to encourage and foster a culture of creativity and originality resulting in a vibrant student and research community empowered with necessary skill sets to provide innovative solutions and breakthroughs. Governmental grants and funding needs to be directly linked with the quantity and quality of patents and research work carried out by these institutions. The industry needs to actively interact and cooperate with the government, academic institutions and R&D organisations so that its products and services are available across the globe at extremely competitive rates. The new age technologies of AI, blockchain and big data have the potential to transform India and propel it to the global fore front of ICT providing nations with a US$ 5 trillion economy by 2025. More than that, it provides it with a strategic leverage and capability to assert and preserve its digital sovereignty.

Notes

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf, accessed on July 5, 2019.
2. To download a copy of Bitcoin open source code go to https://bitcoincore.org/en/download/, accessed on August 9, 2019.
3 From Gartner's Glossary of Terms at https://www.gartner.com/it-glossary/big-data/, accessed on August 14, 2019.
4. Melanie Swan, "Blockchain. Blueprint for a new economy", *O'Reilley Media*, February 2015. A major portion of the concepts of Blockchain have been taken from this book.
5. For more details go to http://www.hashcash.org/, accessed on August 30, 2019.
6. Ana Alexandre, "Japan's national Police Agency to Employ New Software to Track crypto transactions", https://cointelegraph.com/news/japans-national-police-agency-to-employ-new-software-to-track-crypto-transactions, accessed on September 9, 2019.
7 Sarah Durrant, *Understanding the Nexus between Cryptocurrencies and Transnational Crime Operations*, City College of New York at https://pdfs.semanticscholar.org/2dbd/b8eaf77f4d4c0498963985940723f16da807.pdf, accessed on September 9, 2019.
8. Report by the Law Library of Congress titled "Regulation of Cryptocurrency Around the World 20018" at https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf, accessed on September 9, 2019.
9. A major portion of study has been carried out from the US Law Library of Congress Report titled "*Regulation of Crypto currency around the World: June 2018*" at https://www.loc.gov/law/help/cryptocurrency/ accessed on September 19, 2019.
10. RBI press release on "Statement on Developmental and Regulatory Policies" April 5, 2018 at https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=43574, accessed on September 19, 2019.
11. Ibid.
12. For more information at https://libra.org/en-US/, accessed on September 18, 2019.
13. For a detailed description of the DAO hack at https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562, accessed on September 18, 2019.
14. For accessing the white paper at https://web.archive.org/web/20150328054135/https://github.com/ethereum/wiki/wiki/White-Paper, accessed on September 24, 2019.
15. Jordan Robertson and Michael Riley, "The Big Hack : How China used a tiny chip to infiltrate US Companies", *Bloomberg Businessweek* October

4, 2018 at https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies?srnd=businessweek-v2, accessed on September 25, 2019.

16. NASSCOM Avasant India Blockchain Report 2019 at https://avasant.com/nasscom-avasant-india-blockchain-report-2019/, accessed on September 25, 2019.
17. For an introduction to DAG at https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090, accessed on September 25, 2019.
18. Hemlata and Preeti Gulia, "Big data Analytics", *Research Journal of Computer & Information Technology Sciences Volume* 4(2), February 1-4, 2016 at http://www.isca.in/COM_IT_SCI/Archive/v4/i2/1.ISCA-RJCITS-2016-001.pdf, accessed on October 1, 2019.
19. For details on the Apache Hadoop ecosystem at https://hadoop.apache.org/docs/r1.2.1/hdfs_user_guide.html, accessed on October 3, 2019.
20. Bernard Marr, "How much data do we create every day? The mind blowing stats everyone should read" at https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6b1554b160ba, accessed on October 4, 2019.
21. Major portions from "Analytics and data Science Industry in India: Study 2018" by Analytics Lab and *AIM* at https://analyticsindiamag.com/analytics-data-science-industry-in-india-study-2018-by-analytixlabs-aim/, accessed on October 9, 2019.
22. GI Cloud Strategic Direction report at https://meity.gov.in/writereaddata/files/GI-Cloud%20Strategic%20Direction%20Report%281%29_0.pdf, accessed on October 9, 2019.

5. Appraisal of India's Cyberspace Ecosystem

I met many a world leader after becoming the Prime Minister. I have met more than 50 world leaders. Out of those around 25-30 have discussed Cyber Security with me. The entire world is concerned about cyber security… I expect that our [Indian] youth will come up with … innovations for cyber security and lend the world a peaceful sleep

– Shri Narendra Modi
Hon'ble Prime Minister of India

Introduction

Indian cyberspace is growing at an astonishing rate with a projected internet population of 730 million by 2020. We have the third largest internet population after USA and China and our internet population grew six times from 2012 to 2017 at an astonishing CAGR of 44 per cent. It is projected that by 2020, 75 per cent of the new internet users would be from rural India and the country will boast of 175 million online shoppers with 75 per cent of e-commerce transactions happening on mobiles.[1]

The cyberspace ecosystem of a vast country like India includes a number of key components. First, the cyberspace infrastructure. This includes internet and mobile penetration, quality of fixed line and wireless infrastructure, data speeds, social media and e-commerce penetration, etc. Second, cyberspace governance. This includes issues pertaining to governmental policies like: development of cyberspace infrastructure, cybersecurity, frameworks on allocation of spectrum;

introduction of new technologies like 5G, AI, blockchain, crypto currency and Big Data analytics; data localisation; user digital privacy; measures for combating cyber-crime; misinformation campaigns and fake news, etc. Cyberspace governance also includes initiatives taken by the government on international cyberspace policy formulations like norms, regime complex, cyber rules and laws and participation in international forums and committees, dealing with cyberspace related issues and legislations. A major portion of cyberspace governance also deals with multilateral and bilateral treaties and cooperation with different countries and organisations. The third major component of the cyberspace ecosystem is defence of cyberspace infrastructure which includes formulation of policies, establishment of national and regional CERTs and defence of critical information infrastructures like finance, power, nuclear, etc. The fourth component of cyberspace ecosystem is the cyberspace based economy which includes ICT industries, revenues, export and import of cyber equipment and services. The fifth component of the cyberspace ecosystem is cyber-crime. The sixth component of cyberspace ecosystem is cyberspace related skill sets and workforce. This includes higher education, R&D, patents and availability of skilled workforce especially in niche areas of cybersecurity, AI, blockchain and big data analytics. The seventh component of cyberspace ecosystem is cyber laws and lastly cyberwar and deterrence capacity and capabilities and cyber diplomacy.

All components of the cyberspace ecosystem need to develop and grow at an equal pace and in close coordination with each other, in order to truly reap the dividends of a digital nation state. Here, a strong, resilient, all pervasive and safe cyberspace promotes good governance, national security, economy, industry, safety and security.

Appraisal of Indian Cyberspace Ecosystem

Cyberspace Infrastructure: The ITU in its statistical report, "Measuring the Information Society Report Volume 2, 2018"[2] has analysed the ICT infrastructure of 192 countries including India. The report focuses on three major areas namely mobile services, fixed services and government policy. A table from the report shows key indicators along with a comparison between India, Asia & Pacific and the World.

Key Indicators	**India**	**Asia &Pacific**	**World**
Fixed tele subscriber per 100 inhab.	1.7	9.5	13.0
Mobile cellular subscriber per 100 inhab.	87.3	104	103.6
Active mobile – broadband subs. Per 100 inhab.	25.8	60.3	61.9
3G coverage (% of population)	88.0	91.3	87.9
LTE/ WiMax coverage (% of population)	88.0	86.9	76.3
Individuals using internet (%)	34.5	44.3	48.6
Household with internet access	25.4	49.0	54.7
International bandwidth per internet user (kbit/sec)	25.9	61.7	76.6
Fixed broad band subscriber per 100 inhab.	1.3	13	13.6
Fixed broadband subs by speed tiers (% distr.)			
(a) 256 Kbit/sec to 2 Mbit/sec	6.7	2.4	4.2
(b) 2 to 10 Mbit/sec	45.6	7.6	13.2
(c) Equal to or above 10 Mbit/sec	47.7	90	82.6

Source: ITU

The table provides some interesting insights. These are:

- The mobile subscriber base in India is less (87.3 per cent) compared to Asia & Pacific (104 per cent) and world (103.6 per cent). In spite of this, India has the second largest number of mobile phones and smart phones in the world. It is therefore evident that the only available market for mobile phones and smart phones in the world is India.
- Internet access to households and individuals is however lacking and needs to be fast tracked.
- The quality of our internet access in terms of broadband speed is poor with more than half of population having an access speed of 10 MBPS or less. In comparison, more than 80 per cent of the world's population enjoys access speeds of 10 MBPS or more. This is an indicator of the poor quality of infrastructure.

The Digital in World[3] and *Digital in India* report 2019[4] by Hootsuite reveals some interesting trends concerning social media usage, e-commerce activity and mobile usage patterns in India. Details of the same are depicted in the table given below.

Attribute	**Globe**	**India**	**India/ Globe %**	**Remarks**
Population	7.676 billion	1.361 billion	17.73	
Adult literacy rate	86%	69%		
Total internet users	4.388 billion	560 million	12.76	India is first in world for internet growth (+21% YoY)
Active social media accounts	3484 million	310 million	8.89	Second highest growth of social media user (+24% YoY)
Time spent on internet	6:42 hrs	7:47 hrs		
Facebook User	2271 million	300 million	13.21	Max user from India. Highest growth (+3.4 % YoY)
Instagram	894.9 million	75 million	0.83	Second highest Instagram users
YouTube	1,900 million	225 million	11.84	T-Series (second largest subscribers in World) SET India (sixth largest subscribers in world)
Accounts with financial institutions	69%	80%		
Credit cards	18%	3%		

Mobile banking	41%	57%		
Use of Ride hailing apps by internet user	30%	47%		Fourth largest in World
Use of mobile wallets by internet user	37%	47%		
Own crypto currency by internet user	5.5%	6.5%		

The following observations can be gleaned from the above table:

- Compared to our population, we have on average fewer internet as well as active social media users. However, we are the fastest in the world in terms of increasing our internet population (Adding 97,885,001 user in 2018 alone) and second fastest in terms of growth of active social media users (Adding 60,000,000 in 2018 alone).
- Indians have shown an astonishing appetite for internet and social media platforms and this offers an enormous opportunity to the government as well as ICT industry.
- Our poor literacy figures are a cause of grave concern as lack of literacy, which can be considered synonymous to cyberspace literacy, can result in a large segment of the population falling prey to fake news, cybercrime/frauds and financial scams.
- In spite of poor internet speeds, Indians generate the maximum data in the world and spend more time on the internet than the world average.
- Facebook and YouTube are the world's most widely used social media apps. India has the largest user base of Facebook in the world with the highest growth (YoY). In addition, we have second highest growth in the number of Instagram users. Our YouTube channels have some of the largest subscriber bases in the world. This all indicates that India is a major revenue provider for global social media platforms like

Google, Facebook, Instagram, YouTube and WhatsApp. This influence can be leveraged with the global social media companies to provide India specific infrastructure, resource, content and services.

- Indians use more internet linked banking and financial services than the global average. This is a very healthy trend and needs to be encouraged. However, due to our poor literacy percentages, a large number of our internet accessing population becomes susceptible to social engineering and cyber frauds and crimes.
- Indians have shown remarkable digital optimism. They have tremendous faith in digitisation and use of internet and cyberspace to improve services, provide transparency, root out corruption, optimise governance and the distribution of governmental benefits to enhance overall quality of life.

An OFC backbone network is an essential indicator of the overall cyberspace infrastructure available in any country. India has made impressive strides in the last couple of years in improving the OFC network countrywide, especially in the rural areas. The total OFC backbone network of BharatNet in June 2014 was 358 km which has been greatly increased to more than 3,50,000 km till December 2017. However, in comparison with developed countries which have an OFC penetration of 70-80 per cent, India has a penetration of 20-25 per cent. This also assumes greater significance as a high OFC penetration is essential for rolling out a successful pan India 5G network.

The government's National Digital Communication Policy (NDCP) 2018[5] has set some very ambitious goals to be achieved by 2022. These include providing universal broadband connectivity of 50 MBPS to all citizens, connecting all Gram Panchayats with 1 gbps connectivity, providing 100 MBPS broadband on demand to all key development institutions and creation of five million public Wi-Fi hotspots by 2020 and 10 million by 2022. As part of National Broadband Mission, the government is targeting an investment of Rs 7 lakh crore from both the government as well as industry over the next four years (2019-2022).

As per Telecom Regulatory Authority of India (TRAI) report, "Yearly Performance Indicators of Indian Telecom Sector 2018",[6] the total Indian telecom subscriber base in 2018 was 1.197 billion, of which wireless internet subscribers numbered 583 million and wired internet subscribers were 21 million. Over 88.93 per cent of the market share of telecom subscribers is with private operators, while the balance 11.07 per cent is with public sector operators primarily Bharat Sanchar Nigam Limited (BSNL) and Mahanagar Telephone Nigam Limited (MTNL). The average cost to subscriber for 1 GB of wireless data is Rs 11.78 while the average revenue for wireless data per data subscriber per month for the telecom subscriber was Rs 90.02. It is clear from the above that India has one of the cheapest wireless data rates in the world, primarily due to its large subscriber base. However, the Indian consumer does not spend much on his wireless data consumption, which leads to intense competition amongst the players, who at times fail to compete amongst each other and are driven to bankruptcy or into mega mergers and acquisitions, in order to remain relevant. Another interesting statistic is that India has an urban tele density of 159.98 per cent and a rural tele density of 59.50 per cent. It is obvious that providing telecom services to a rural subscriber base at the same or lower tariff, as to an urban subscriber base will greatly affect the telecom service provider's margins. The PSU, BSNL has been the primary provider of telecom services to rural India. This coupled with an excessive work force and out dated technology has resulted in the company making huge losses and going into the red. The private players are not doing that great either. Barring Reliance Jio, which has emerged as market leader in just three years with a subscription base of 331.3 million, the rest of the major players have lost out on the subscriber base and revenues and have merged with one another. Major mergers in the telecom sector are Vodafone with IDEA and between Bharti Airtel and Telenor. The Adjusted Gross Revenue (AGR) in 2018 was Rs 1,44,446 crore which was -10.18 per cent less that the AGR of 2017.

In the quarter ending September 2019, Vodafone IDEA posted the country's largest quarterly loss of Rs 50,921 crore and Bharti

Airtel posted a loss of Rs 23,045 crore in the same quarter. In addition, the government has decided to merge BSNL and MTNL and offer a Voluntary Retirement Scheme (VRS) to thousands of employees, in order to resurrect the failing mega PSU companies. In such a scenario, providing state of art digital infrastructure at extremely competitive rates, becomes a major challenge for the service providers.

Data Centres are another critical component and significant indicator of the overall cyberspace infrastructure in a country. Data centres are typically classified according to their types or *tiers*. A *Tier 1* Data Centre is a basic data storage solution which does not provide back up to power and cooling failures. Typically, they are less stringent regarding Quality of Service (QoS) parameters and have a minimum uptime of 99.67 per cent and 28.8 hours of acceptable annual downtime. A *Tier 2* Data Centre has partial redundancy systems in place with a minimum uptime of 99.741 per cent and 22 hours of acceptable annual downtime. A *Tier 3* Data Centre has the basic data centre configuration for enterprise solutions. They have inbuilt redundancies to cater for equipment, power and cooling system failures and also for operational contingencies. In addition, both UPS and generators are available for providing a two layered back up for power systems. They have a minimum uptime of 99.982 per cent and 1.6 hours of acceptable annual downtime. A *Tier 3* Data Centre has N + 1 redundancy where in N refers to the total number of essential equipment and systems required to run the Data Centre. A *Tier 4* Data Centre truly incorporates a full system failure tolerance and has a 2N redundancy. This implies that each component of Data Centre is duplicated (one in running and one in hot standby mode), much akin to having two engines in an aircraft. These data centres have a minimum uptime of 99.995 per cent and 0.4 hours of acceptable annual downtime.

There are five major requirements for having state of art large scale data centres in India. First, there is a growing business opportunity for cloud hosting and applications. Second, the draft data laws and policies of the government hint at ensuring data localisation of at least the critical data, which has been generated within India. Third, a large number of multinational ICT companies have realised the enormous opportunity offered by providing cloud based services from within India and have established local data centres, like Alibaba has established in Mumbai in January 2018. Fourth, e governance initiatives taken by the government as part of digital India for providing a large number of services and direct benefit transfers to citizens; and lastly, the internet consumer base coupled with data generation is growing exponentially requiring new data centre to handle, manage and analyse the generated data.

The global data centre market was a $170 billion market in 2017 of which the market share of the US alone was 40 per cent ($68 billion); followed by EU and Russia (32 per cent ($54 billion)); Asia Pacific Region 25 per cent, ($42 billion); and lastly Middle East and Africa three per cent, ($6 billion). In 2017, India's share of the global data centre market was around $1.3 billion which is expected to reach $4 billion by 2024. India is the second largest market for Data Centre infrastructure after China in the Asia Pacific region.

As per world data centre map,[7] presently there are 152 data centres in India with bulk of them in New Delhi (16), Bangalore (26), Chennai (13), Hyderabad (10) and Mumbai (24). The present data centre capacity in India is quite low when compared with our active internet population and quantum of data being generated within the country. With an active internet population of 560 million users, we have less than 700 Mega Watt (MW) capacity of data centre in India, whereas Europe, which has an active internet population of 460 million, has a data centre capacity of 8600 MW.

Cyberspace Governance: The Ministry of Communications and Ministry of Electronics and Information Technology (MeitY) are the two ministries primarily dealing with all aspects of cyberspace governance in India. The erstwhile Ministry of Communications and Information Technology was bifurcated into the above two ministries in July 2016.

The Ministry of Communication comprises of the Department of Telecommunication (DOT)[8] which is responsible for policy, licencing and coordination matters, relating to telecommunications within India, as well as international cooperation with a large number of telecommunication related organisations and bodies like ITU, International Telecommunication Satellite Organisation (INTELSAT), International Mobile Satellite Organisation (INMARSAT) and Asia Pacific Telecommunication (APT). It is also responsible for promoting telecommunication standards as well as R&D, in this field. The Ministry of Communication has two statutory bodies under it namely, the Telecommunications Regulatory Authority of India (TRAI) and Telecom Disputes Settlement and Appellate Tribunal (TDSAT). It also has two public sector telecommunication companies under it (Bharat Sanchar Nigam Limited (BSNL) and Mahanagar Telephone Nigam Limited (MTNL)).

The major charter of MeitY includes policy matters relating to IT, electronics and the internet, matters relating to cyber laws, as well as other IT related laws, promotion and manufacturing of semiconductor devices, coordination with various international agencies dealing with IT related matters, promoting standardisation, testing and quality of IT products and services. It has three statutory bodies under it, namely, Controller of Certifying Authority (CCA), Indian Computer Emergency Response Team (ICERT) and Unique Identification Authority of India (UIDAI).

India has multilateral cooperation in the field of IT, with a number of countries and has signed Memorandums of Understanding (MOUs) with almost 50 countries. These MOUs primarily involve setting up of IT related Centres of Excellence, assistance in undertaking welfare projects like tele medicine facilities, e prison etc., sharing of best practices and enhancing IT education and literacy. What is important is that the ICERT has signed MOUs with its counterparts in seven countries namely Australia, Bangladesh, Canada, Japan, Singapore, USA and Uzbekistan for mutual cooperation relating to exchange of information and any threats with each other. However, it is felt that there is a need for more CERT based intelligence sharing and cooperation treaties with a number of nations and organisations, especially with those in our neighbourhood. A comprehensive cyber security treaty amongst all the member countries of Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) namely Bangladesh, India, Myanmar, Sri Lanka, Thailand, Nepal and Bhutan is an urgent necessity.

The government has brought into force the IT (Amendment) Act of 2008, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016, the MeitY Business rules, IT (Information Security Practices and Procedures for Protected System) Rules, 2018 and a large number of policies and guidelines, especially in the past five years. Notable among the are: National Data Sharing and Accessibilty Policy (NDSAP); National Cyber Security Policy (NCSP) 2013; National Policy on Software Products 2019; Policy on adoption of open source software for Government of India; National Policy on Universal Electronic Accessibility; guidelines on adoption of electronic payments and receipts, guidelines for publication of e books; and guidelines for strategic control in outsourced projects. However, a large number of key legislations have not seen the light of the day even when the draft legislations have been received after going through iterative processes with the general public and affected businesses and organisation. Notable amongst them are: the Justice BN Srikrishna committee draft "Personal Data Protection Bill, 2018"[9] submitted to the government on July 27, 2018; the Draft National e-Commerce Policy; intermediary guidelines rules; laws on curbing of fake news and misinformation campaigns; and use of dual use technology like AI in defence and other strategic sectors. The NCSP is of 2013 vintage and does not fully address the changed reality of the cyberspace domain of 2020. The National Cyber Security Coordinator (NCSC) has stated on record that a new National Cyber Security Policy will be released in 2020.

The absence of laws, policies and rules has major ramifications. India presently lacks data privacy laws. Recently, Yahoo reached a $117.5 million class action settlement concerning its 2013 data breach in which nearly three billion Yahoo accounts had been compromised. Users affected by the breach can get payments ranging from, $100 to $358, depending on the number and types of claims filed against the company.[10] However, due to the lack of a data privacy law, Indians are unable to sue ICT companies over loss of private digital data.

The second issue affecting non availability of laws and rules is the environment of opacity and lack of clarity, wherein large corporations find it difficult to take strategic decisions concerning investments and collaborations within India and its business entities.

Lastly, in spite of existing laws and regulations, the government finds it increasing difficult to get them implemented by multinational companies who lack a major physical presence within the territorial jurisdiction of India. A recent case in point is the end to end privacy feature offered by number of messaging apps like WhatsApp and Telegram. Though, section 69B of the IT (Amendment) Act 2008 and IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 gives the central government the power to monitor and collect traffic data, it is unable to make global multi national ICT companies comply with the law. Global messaging companies like WhatsApp and Telegram counter that since their messaging platforms are end to end encrypted, with the private keys being stored in the user's smart phone/computer only, it is impossible to intercept the content of the messaging between individual users. Telegram even has a $300,000 reward for anyone who can intercept and decrypt their end to end messages.

Another issue related to cyberspace governance is that owing to the nature of domain (highly complex, fast evolving, global, multi-disciplinary and dual use), it is always better to have centralised control with decentralised execution. Thus a single ministry (say, Ministry of Cyberspace) would be able to better control and coordinate the multiple requirements of various stakeholders, than two ministries. This would ensure that everyone is on the same page with a single point of contact in the government and lastly that the critical human resource (which is always in short supply) is optimally utilised and employed.

Government Initiatives and Digital Reforms: MeitY in its report titled "India's Trillion-Dollar Digital Opportunity"[11] has elaborated on a number of initiatives and reforms undertaken in the past few years to ensure that ICT technology is affordable, inclusive and transformative along with the Digital India programme that aims at transforming India into a knowledge based economy and a digitally empowered society.

Aadhaar has been successful in providing digital identity to 123 crore people with 99 per cent coverage of adult population. From 2014 to 2018, under the Aadhaar based Direct Benefit Transfer (DBT), Rs 6.21 lakh crore have been disbursed to the beneficiaries of 438 government schemes resulting in a savings of Rs 1.1 lakh crore, following the deletion of fictional accounts. The digital payment transactions have also grown manifold with 67 crore transactions in January 2019, valued at over Rs 1 lakh crore.

One of the most significant initiatives taken by the government is the proposed India Enterprise Framework.[12] The implementation of this framework will ensure optimised delivery of high quality government services in a highly complex and heterogeneous environment. The India Enterprise Architecture (IndEA) envisages a federated architecture wherein the client entities (could be states, UTs or other governmental organisations) would have their own customised solutions for delivery of e-government services, in keeping with the principles and standards of IndEA. This will ensure pan India interoperability and constitute a network of networks capable of providing quality and quantity of services using optimum resources.

Another key initiative taken by the government is the digital delivery of services. The National Scholarship portal has 1.40 crore registered students and scholarships worth Rs 5395 crore have been disbursed from 2015 to 2018. Since 2014, 2.48 crore Digital Life Certificates have been submitted online by pensioners. Digilocker is providing access to over 349 crore certificates in digital format and the Unified Mobile Application for New Age Governance (UMANG), provides a single digital platform to the citizen to access over 339 different government schemes. The government has opened 3.12 lakh Common Service Centres (CSC) to deliver doorstep e-services. This has generated employment for over 10 lakh people of which 54,800 are women. Under the Pradhan Mantri Digital Saksharta Abhiyan, which is the world's largest digital literacy mission, already 1.96 crore persons from rural areas have been made digital literate.

The government is eyeing the BPO sector, which has the potential to generate 1.5 lakh employment opportunities in smaller towns across the country. Already, 268 BPO units have been established at 110 locations with 53,300 seats allocated to 184 companies.

Under the Make in India, Make for India and Make for World initiative of the government, a total of 268 mobile and mobile component manufacturing units have been set up between 2014 to 2018. This has resulted in direct and indirect employment for 6.7 lakh people.

Defence of Cyberspace: The defence of the Indian cyberspace is a shared responsibility of the National Cyber Security Coordinator (NCSC), CERT-In, NCIIPC, Defence Cyber Agency (DCA) and the cyber security teams of all three defence services.

In March 2015, the Government of India created the post of NCSC under the National Security Council Secretariat (NSCS) who would coordinate cyber security related matters amongst the various ministries and stakeholders.

The CERT-In acts as a single point resource for reporting, analysing and responding to any cyber incident within the country except for critical information infrastructures. The major tasks of CERT-In are to provide a 24x7 security service for cyber threats reporting and response. Second, issue security guidelines and advisories from time to time. Third, act as a central repository for cyber intrusions within the country. Fourth, carry out risk and vulnerability analyses and lastly training other cyber security agencies as well as coordinating with international CERTs and other cyber security agencies.

In August 2017, the government established the National Cyber Coordination Centre (NCCC) under CERT-In. The NCCC is a multi-stakeholder organisation, capable of scanning meta data and web traffic to detect cyber security threats, in real time. Another initiative taken by CERT-IN is the Cyber Swachhta Kendra which is a Botnet cleaning and Malware analysis centre. The Cyber Swachhta Kendra provides information on security best practices, cybersecurity alerts and a host of security tools, including a free Bot removal tool from Quick Heal.

In 2018, CERT-In handled 2,08,456 incidents ranging from website intrusion and malware propagation, malicious code, phishing, DDoS attacks, website defacements, unauthorised scanning activities and vulnerable services.[13] India is the second most cyber targeted country in the world after USA with almost 17 per cent of the total worldwide attacks being targeted at India.

The ITU publishes a yearly Global Cyber Security Index as a measure of the commitment of countries to cyber security. The assessment is carried out along five verticals namely, legal, technical, organisational, capacity building and cooperation, which is then aggregated to arrive at the overall score and determine global ranking of each country.

The Global Cyber Security Index of 2017 of 134 countries placed India at number 23. India was ranked 47 among 193 countries in 2018. There is no denying the fact that a modern, resilient and safe cyberspace ecosystem is a strategic imperative if India is to achieve its aim of becoming a $5 trillion economy by 2025. It is also important for the success of the flagship Digital India programme with its vision of transforming the country into a digitally empowered society and knowledge economy.

The NCIIPC is a unit of National Technical Research Organisation (NTRO) which directly comes under the National Security Advisor (NSA). The NCIIPC acts as the national nodal agency to protect Critical Information Infrastructure (CII). Its major charter includes the coordination, sharing, monitoring, collecting, analysing and forecasting of national level threats of the CII. The basic responsibility for protecting the CII systems lies with the agency running the CII. Also, as per its charter, the NCIIPC is not responsible for the audit of CII systems.

The CII has broadly been classified into five major sectors – power and energy, banking, financial institutions and insurance, ICT, transportation and e-governance and strategic public enterprise. The defence and intelligence agencies networks have been kept out of the purview of NCIIPC.

In May 2018, MeitY promulgated the rules for Information Security Practices and Procedures for Protected Systems.[14] As per the above rules, each organisation with a "Protected System" will constitute an Information Security Steering Committee (ISSC) which will also have a representative from NCIIPC. The organisation shall nominate a Chief Information Security Officer (CISO) and field its system and carry out various procedures as per guidelines and Standard Operating Procedures (SOP) laid out by the NCIIPC from time to time. The organisation will conduct periodic internal as well as external audits and establish a Cyber Security Operation Centre (CSOC) and a Network Operating Centre (NOC). Presently the TETRA secured communications system network, the Central Identities Data Repository (CIDR) of UIDAI, Long Range Identification and Tracking (LRIT) system of the Ministry of Shipping and the Goods and Services Tax Network (GSTN) database are protected systems in India.

Establishing and running a critical information network is similar to the construction and maintenance of a multi storied specialist building like a hospital, etc. In the case of a specialist building, before start of construction, the plans need to be verified and approved by multiple regulators. During construction, regulators carry out periodic inspections to ensure that construction is being carried out as per plans, using correct materials and processes. Before giving out the occupation certificate, the regulators again conduct inspections and satisfy themselves about the quality of construction and safety of structure. Finally, periodic inspections and certificates are issued by regulators at pre designated intervals during the entire lifecycle of the building.

Similarly, before the fielding of a critical information network, the plans and procedures of the network need to be vetted and cleared by an appropriate agency like the NCIIPC and thereafter, regular inspections need to be carried out by third party inspectors, to ensure that the network is being fielded as per specifications. It should be ensured that the procedures for safety of information and resources are in place and being adhered to, in letter and spirit. Finally, regular audit and certifications need to be carried out during the entire lifecycle of the network. Any fresh addition to the infrastructure or replacement of existing equipment and application, needs to be first vetted and approved by NCIIPC, prior to its fielding.

Though the rules for Information Security Practices and Procedures for Protected Systems streamline a number of aspects relating to protection of CIIs, but they are more or less lacking in finer details and the nuts and bolts. It is also important that the accountability and responsibility between the organisation fielding the "Protected System" and NCCIPC be clearly demarcated to avoid any misunderstanding or confusion, in case of a major failure or breach. Third, it is important that the external audit of all "Protected Systems" be carried out by NCIIPC or through its nominated auditors, as part of a Public Private Partnership (PPP) model. Recently, the US Department of Homeland Security vide the US "Department of Homeland Security (DHS) Cyber Hunt and Incident Response Team Act of 2019"[15] created a permanent team of cyber security professionals that is available 24x7 at the US Cybersecurity and Infrastructure Security Agency to act as immediate responders against any attack on the state or private information systems. Such high level empowered teams need to be created and stationed at both the central, as well as at sectoral and regional CERTs and NCIIPC.

The US has a detailed and well documented system for procurement, security, management, standardisation and risk management framework for their governmental ICT assets. The FISMA act of 2014 along with NIST standards as well as Circular A-130, give exhaustive details of procedures, standards and responsibilities with regard to the use of ICT resources by the US governmental agencies. This is absent in the Indian context.

Another aspect which needs to be considered is that CERT-In and NCIIPC work under a different ministry/organisation. There would be greater coordination, focus and optimisation of skilled manpower and resources if both these agencies were placed under one agency, namely NTRO. This is because the NTRO has a wider technical resource base and skill set and would be able to respond better to the growing threats to our national cyberspace ecosystem, since it operates under the NSA.

Indian Common Criteria Certification Scheme (IC3S):[16] The Common Criteria for Information Technology Security Evaluation (CC) and Common Methodology for Information Technology

Security Evaluation (CEM) are part of the international Common Criteria Recognition Arrangement (CCRA) with 17 Certificate Authorising members (including India) and 14 certificate consuming members. The aim of CC is to get IT products evaluated by competent and independent licenced labs and the certification be recognised by all CCRA countries.

The Standardisation Testing & Quality Certification (STQC) is a quality assurance agency of MeitY which aims to establish a certification body and test lab for evaluation and certification of IT products. There are four types of Evaluation Assurance Level (EAL) certifications from EAL 1 (basic) to EAL 4 (best). The EAL 1 is tested functionally, EAL 2 structurally, EAL 3 methodically while EAL 4 is methodically designed, tested and reviewed.

STQC has four certification labs at Kolkata, Delhi, Bengaluru and Mumbai where 12 IT products have been certified, till date. It is evident that the certification infrastructure available in the country is inadequate to meet the growing demands of our digital nation. Also, providing certification is a niche capability, which has the potential to generate a large revenue both within as well as outside the country.

Cyberspace Based Economy: The broad categories of ICT industry include software, devices and infrastructure, IT and business services, emerging technologies and telecommunication services. By 2019, the global ICT market including video and TV services are projected to be a €4.4 trillion industry.[17] The Indian ICT sector is expected to have revenue of $225 billion by 2020 with a growth CAGR of 11.1 per cent.[18] In addition, as per United Nations Conference on Trade and Development (UNCTAD) statistics of 2017,[19] India had a negative trade balance of –$147,840 million in spite of an export growth rate of +13.3 per cent.

India is a signatory to the Information Technology Agreement (referred to as ITA-1), which is a plurilateral agreement of World Trade Organisation (WTO). A total of 82 member countries accounting for nearly 97 per cent of world trade in IT products, are signatories of ITA-1. Since 2012, a number of developed member countries (primarily US, EU and Japan) of ITA-1 have been proposing to broaden the scope and participation of ITA-1. Proposals include increasing the coverage of IT products with zero customs duty, addressing non-tariff measures and increasing the number of signatory countries. India considers the proposals of ITA-2 detrimental to the government's domestic manufacturing initiatives and has therefore has decided not to participate in ITA-2 discussions.

The Department of Commerce in its annual report for 2018-19[20] has stated that in spite of a challenging global market environment, the Indian exports have been growing steadily since 2016-17. They crossed the $500 billion mark for the first time in 2018-19 with a YoY growth of 7.47 per cent. The services sector in India has traditionally being registering a growing trade surplus between imports and exports. In 2018-19 the trade surplus was $80.3 billion compared to $77.6 billion in 2017-18 and $68.3 billion in 2016-17. The services trade surplus is responsible for reducing almost half the negative trade surplus in the merchandise sector. Another major takeaway from the report is that Special Economic Zones (SEZ) have played a key role in attracting investments, creating jobs and promoting exports.

India is striving to become a $5 trillion economy by 2025, of which the services sector share is estimated to be $3 trillion. Since, the services sector has been consistently performing well in comparison with other sectors, the government has decided to launch a Champion Services Sector Scheme (CSSS) to encourage diversification and quick expansion of the sector, which is presently primarily focused on IT and Information Technology Enabled Service (ITeS). In line with this, the Department of Commerce cabinet note on "Action Plan for Champion Sectors in Services" was approved by the Union Cabinet on February 28, 2018. The CSSS is proposed to have a dedicated fund of Rs 5,000 crore to support sectoral initiatives in 12 priority sectors. These are: IT & ITeS; Tourism and Hospitality Services; Medical Value Travel; Transport and Logistics Services, Accounting and Finance Services, Audio Visual Services, Legal Services; Communication Services; Construction and Related Engineering Services; Environmental Services; Financial Services; and Education services.

The government has listed 30 digital schemes in nine key areas, which if scaled up nationally have the potential to create a trillion dollar economic value by 2025. These schemes are:

- **21st Century Infrastructure and Software Capabilities:** Equipping IT-BPO industry with digital technologies of future, creating state of art cybersecurity and data protection frameworks, building capabilities for real time data visualisation and data analytics and broadband for all.
- **E-Governance for the Future:** Scaling up the government e-marketplace, a comprehensive DBT, Digital land 2.0 to digitise land records, creating a national document and data exchange, introducing shareable APIs and tools for improved e-governance and providing Common Service Centres in all gram panchayats.
- **Healthcare For All:** Creating a Universal Health Record (UHR) for all, providing technology enabled remote healthcare and offering a universal public health insurance platform.
- **Quality Education for All:** Promoting digital content delivery and creating an integrated education content platform.
- **Energy for All:** Expanding digitally enabled affordable power access to include digital pre paid meters, digitised billing, advanced power analytics etc. and creating smart grids to integrate distribution generation and renewables.
- **Next Generation Financial Services:** Encouraging a cash less economy and introducing flow based lending and advanced credit underwriting, through data driven credit evaluations.
- **Doubling Farmers Income:** Enabling digital financing and insurance pay outs, introducing precision agriculture and implementing online marketplace.
- **Make in Digital India, Make for India, Make for World:** Facilitating end to end supply chains, e-enabled trade and e-commerce, efficient passenger transportation, fostering an integrated logistics platform, encouraging manufacturing automation and IoT based advanced analytics and building a vibrant electronic device manufacturing ecosystem.
- **Jobs and Skills for All:** Skill building for the future, creating an online talent marketplace and promoting digitally enabled jobs.

The above schemes are a major indicator of the government's vision and intent to usher in an enabling digital environment and ecosystem across the country, which would greatly enhance the nation's economy, agriculture, industry, education and overall ease of working and living. However, the taste of the pudding lies in its eating and a lot will depend on the scale, quality and timing of implementation.

Cyber Crime: As per National Crime Records Bureau Statistical publication *Crime in India 2017,*[21] a total of 21,796 cyber crimes were reported in India in 2017, which is a 77 per cent increase from the cyber crimes reported in 2016 (12,317 cases). On an average, there were 1.7 cyber crimes reported per one lakh population, in 2017. Fraudulent transactions and sexual exploitation were the most widely reported cases, with 12,213 cases of cyber fraud and 1,460 cases of sexual harassment and exploitation, registered in 2017.

Among the metros, Bengaluru reported almost twice the number of cyber crime related First Incident Reports (FIRs) filed in 2018 as compared to 2017. A total of 5035 FIRs were filed in 2018, but due to a lone and under staffed police station dealing with cyber crime, there was a marginal drop in the number of charge sheets filed during both the years.[22]

Ministry of Home Affairs (MHA) created a Cyber and Information Security (CIS) Division headed by a joint secretary in 2017. The CIS division is responsible for implementation of National Information Security Policy & Guidelines (NISPG) by all government ministries and departments. These include: cyber security and risk assessment of IT infrastructure of various government ministries/departments and organisations; coordination in fighting cyber-crime; oversee schemes for prevention of cybercrimes against women and children; establishing the Indian Cyber Crime Coordination Centre (I4C) and National Cyber Forensic lab (NCFL); carryout regular information security audits of various ministries/departments; participate in international conventions on cyber security and cyber crime; and be responsible for lawful interception and functioning of National Intelligence Grid (NATGRID).

In February 2019, the NCFL and Cyber Prevention, Awareness and Detection (CyPAD) centre was established in New Delhi. In addition to the NCFL, the Central Forensic Science lab, Hyderabad also has a Computer Forensic Unit. The NCFL has a memory forensics lab, image enhancement labs, crypto currency forensic labs, damaged hard disks and advanced mobile forensic labs. In addition, the Government of India in a series of gazette publications in 2018, designated the Cyber Forensic lab, Army Cyber Group, Computer Forensic and data Mining Lab and Forensic Science lab, as examiners of electronic evidence.

The I4C consists of seven verticals. These are: National Cyber Threat Analytics Unit (TAU); National Cybercrime reporting; Joint cybercrime investigation team; National Cybercrime Forensic laboratory ecosystem; National Cybercrime Training Centre; Cybercrime Ecosystem Management unit; and National Cyber Research and Innovation Centre. In addition, funds have been released to all states and union territories in 2018 to establish forensic units and capacity building units for the collection, preservation and analysis of digital evidence and to skill police personnel, prosecutors, judges and other law enforcement personnel for dealing with cases pertaining to cybercrime.

India has one of the largest and fastest growing user bases of internet, social media and messaging apps. In addition, the first time users of smartphones, mobile banking apps, social media and messaging services are predominantly women and from rural areas. The above creates a deadly cocktail which is highly susceptible to identity thefts, financial scams, fake news, misinformation campaigns and internet addiction. A case in point is the July 1, 2018 incident at Rainpada village of Dhule district, where five tribals were killed by a mob, on the basis of rumours, that they were child lifters, were circulated on social media. Thus, the miniscule number of reported cyber crime figures of 2017, raises a red flag that a large number of cyber crimes, especially those pertaining to financial fraud, identity theft and sexual harassment had been left unreported. In addition, the fall in the number of FIRs filed in cases pertaining to cyber crimes along with the miniscule percentage of police personnel trained for cyber investigations and forensics, will make India a lucrative territory for cyber criminals.

A major initiative taken by the government to increase the number of FIRs pertaining to cyber-crimes is by the launching of a comprehensive cyber-crime portal[23] which makes it much easier to report a host of cyber-crimes across the country, without stepping into any police station. This would definitely encourage citizens as well as enforcement agencies to report, detect and fight cybercrime, in a more focused and optimum manner.

Cyber security education is an extremely niche and exclusive skill set which is acquired after years of training and on the job exposure. Though, a large number of organisations, institutes, labs and schemes have been launched by the government in the past few years, their impact will only be felt, once they get fully established and have the requisite professionals with the right skill sets required to combat cybercrime.

Cyberspace Related Skill set and Workforce: There are 993 universities, 39,931 colleges and 10,725 standalone institutions offering higher education in India. Of these, 16 universities are exclusively for women. On an average, India has 28 colleges per 1 lakh eligible population.

The All India Survey on Higher Education (AISHE) 2018-19[24] report of the Ministry of Human Resource Development (HRD), provides extensive data on the various indicators of higher education in India. Details of the same are given in the succeeding paragraphs.

The total enrolment in higher education is 37.4 million students. Of these, females constitute 48.6 per cent and the share of undergrad enrolment is 79.76 per cent. Bulk of the enrolment at the undergrad level is in the humanities stream with a 16.5 per cent enrolment in the science and 13.5 per cent enrolment in the engineering and technology streams. In 2018, 21.25 lakh students enrolled for B Tech courses while 16.45 lakh students enrolled in for BE courses.

A total of 47,427 foreign students from 164 countries are enrolled in India. Most foreign students are from Nepal (26.88 per cent), Afghanistan (9.8 per cent), Bangladesh (4.38 per cent), Sudan (4.02 per cent), Bhutan (3.82 per cent) and Nigeria (3.4 per cent).

A total of 3880 students are enrolled in integrated PhD and 1,69,170 enrolled in PhD. In 2018, 40,813 students were awarded PhD degrees. At PhD level, maximum students are from Engineering and technology stream (41,869) followed by Science Stream (5848).

The SCImago Journal & Country Rank is a public portal, that includes the journals and country scientific indicators developed from the information contained in the Scopus[25] database. India with 16,70,099 international published citable documents ranks overall 9th in the country rankings with USA (1,20,70,144) and China (59,01,404) in the first two places respectively. The above rankings are a reasonable indicator of the overall level of research being carried out in a particular country. What is surprising is that countries like UK, Germany, Japan, France, Canada and Italy are ranked higher than India, in spite of having significantly lower number of students pursuing higher education and fewer universities, colleges and institutions of higher education. India's rankings improve slightly in case of STEM subjects, namely computer science (7th rank), Decision Science (6th rank), Engineering (6th rank) and Maths (10th rank).

As per World Intellectual Property Organisation (WIPO) statistics, India's share of international patents grew one and half times from 11,939 in 2009, to 30,036 in 2018.[26] The WIPO report titled "World Intellectual Property Indicators 2019"[27] gave details of the global trends in patent and trademark filings in 2018. A total of 3.3 million patents (growth of 5.2 per cent compared to 2017) and 14.3 million trademarks (growth of 15.5 per cent over 2017) were filed in 2018. China accounts for the maximum number of patents and trademarks filed globally in 2018 with the IP office of China accounting for 46.4 per cent of all patents and 51.4 per cent of all trademarks filed in 2018. The patents and trademark filing in China in 2018 saw a remarkable increase of 11.6 per cent and 28.3 per cent respectively compared to 2017. India ranked 10th in the world with the individual ranking of 12th in patent, 9th in trademark and 13th in industrial design filings. Among the top twenty ranked countries, India demonstrated the fourth largest year on year growth with an increase of +7.5 per cent over 2017.

The Patent Cooperation Treaty (PCT) of WIPO allows an applicant to file a single international patent which provides patent protection across a number of countries. In 2018, approximately 2,53,000 PCT patent applications were filed. Of these, China, India and Turkey were the only three middle income countries featuring in the top twenty patent filing nations and India with a YoY growth of +27.2 per cent recorded the highest growth amongst all PCT patent filing countries.

The rapid proliferation of internet coupled with IoT devices, mobile banking, smart technologies and solutions across the globe, will create a huge demand for a workforce that is highly skilled in latest cyberspace technologies of cybersecurity, AI, blockchain and big data analysis. In fact, with a large English speaking STEM population, India is suitably poised to become the world leader in these highly rewarding, non-manufacturing, non-polluting high tech cyberspace industries of tomorrow. The moot question is that do we have the requisite infrastructure, ecosystem and skill set in required numbers to become the leader of next generation innovative and highly rewarding industry of the future?

Cyber Laws: The IT (Amended) Act 2008 is the latest legislation pertaining to cyberspace in India. There have been a number of policies and procedures promulgated by the government in recent times, but these cannot be considered as truly empowering. There is an urgent requirement to introduce new legislation and amend the existing IT (Amendment) Act 2008 as a large number of changes have taken place in the cyberspace domain since 2008.

Fake news and misinformation campaigns have been the hot topics of debate the world over. The revelations by 28 year old Christopher Wylie in March 2018 concerning the role of Cambridge Analytica, in harvesting millions of Facebook users data to create sophisticated psychological and political profiles in order to create targeted political ads during the US presidential elections, opened a can of worms which led to the firm being investigated by both US (Special Counsel Robert Mueller's investigation) and the UK (Electoral Commission for role in EU referendum and Information Commissioner's office, for carrying out data analytics for political purposes).

Another important aspect of internet based messaging is the end to end encryption and traceability of messages. A number of messaging sites such as WhatsApp and Telegram have proclaimed that they use highly secure end to end encryption with the private key being stored only in the end user smartphone or terminal and that messages between various users and groups cannot be traced. This provides space to criminals and people/ organisations/ states with nefarious designs and plans to spread fake news and conduct misinformation campaigns.

In a written reply to the Rajya Sabha on November 21, 2019, the Hon'ble Minister of State for Electronics and IT stated that the government was in the process of finalising new rules for social media companies (also called internet intermediaries), that would require traceability of originator of information and removal of malicious content within 24 hours of notice.

The Hon'ble Supreme Court has declared that privacy is a fundamental right of a citizen. The growing use of social media, financial and other similar platforms that require users to store their personal information and content, the safeguarding and lawful use of this storehouse of digital Personal Identifiable Information (PII) becomes of paramount importance. A large number of legislations like the EU's GDPR require internet intermediaries as well as Internet Service Providers (ISP) to take consent, handle and safeguard user personal information in a transparent and well defined manner. Also adequate penalties have been built into the legislations to force companies to take user privacy seriously.

In India, a large number of important draft legislations are being processed by the government with delays running into months and sometimes years before they finally get enacted into law. Notable amongst these are the Justice B.N. Srikrishna Committee Report on Data Protection Law[28] (submitted in July 2018), Draft Intermediaries Guidelines (Amendment) Rules 2018[29] (Submitted in December 2018), Draft National Policy on encryption (submitted in September 2015) and Draft National e-Commerce Policy[30] (Submitted in February 2019). Cyberspace is a domain where the pace of change is global and fast. Any delay in bringing out empowering legislations costs both the citizens as well as the government and provides intermediaries additional time to monetise individual PIIs without fear of law in any manner and maximise their profits.

Cyber War, Deterrence Capacity and Capability: The Indian Armed Forces raised the DCA in May 2019 at Delhi. The agency is a triservices organisation headed by a two star ranked officer. The exact nature, organisation, tasks and scope of work of the newly created agency are not available in the public domain and are subject to speculation. The creation of the post of Chief of Defence Staff (CDS) by the government along with the creation of DCA, Defence Space Agency and Special Forces Division is an indicator of the government's intent to usher in a greater degree of jointness amongst the three services.

One of the key tasks of the DCA would be to protect the critical networks of all the three services as well as those directly under the MoD. In addition, the agency could also be tasked to ensure that service personnel do not fall prey to adversary's misinformation campaigns as well as efforts to honey trap them, by using social media and other internet propagated means. Information security of digital data stored on the service cloud, as well as within defence networks, could also be one of the important tasks entrusted to the DCA. Carrying out regular performance audits and testing of network procedures and response under attack and sabotage could well be another task that could be allocated to the DCA. In addition, certain offensive tasks including cooperation and information exchange and assistance with friendly foreign countries could be given to the agency.

There will be a number of challenges which the DCA would be required to overcome as it goes about providing a fully secure cyberspace domain for the Defence Forces. First, the three services networks need to be fielded, integrated and managed by a single agency. This is not only critical for standardisation and interoperability but also extremely important from the cyber security point of view. It is assumed that the DCA would not be mandated for fielding and manning the network but would be responsible for its defence and audit. Thus, it would be necessary that the network being fielded be first vetted and cleared by the DCA prior to being implemented on ground. Second, all network security procedures, protocols and maintenance schedules as well as network redundancies be again cleared and vetted by the DCA. Herein lies the first challenge. True jointness in fielding, managing and protecting the cyberspace can only come about once there is a single agency or organisation mandated to provide the common cyberspace to all the three services, with service specific segregation being implemented using a host of technological means like virtualisation and segmentation. Presently, all the three services implement, manage and audit their networks separately.

Second, the organisation providing the common network to the three services needs to be an inter service organisation, directly under the CDS. Then only can the two tasks of network provisioning and its defence and audit be performed satisfactorily, with a single head responsible and accountable for any failure and sub optimal performance of the network, when it is subjected to overload and attack in times of crisis.

The third important challenge which needs to be overcome is the formulation of a common cyber doctrine, procedures and protocols. In addition, the training and trade structures of personnel responsible for fielding, managing and auditing the networks, need to be common to all. Lastly, there should be standardisation and an equipment testing agency not only for defence but for all equipment and applications supplied to critical Information Infrastructure networks. Important lessons can be gleaned from the model implemented by the US of NIST and Defence Information System Agency (DISA) which is responsible for the information infrastructure provided not only to the various defence services but also to President, Vice President, Secretary of Defence and any other agency, as declared from time to time.

Cyber Diplomacy: It has been well established that India is a major stakeholder in the global cyberspace domain and it needs to play a major role in formulating global cyberspace strategies, laws and policies especially those like the UN led global cyber norms on which a number of GGEs have been held.

Formulation of global cyber norms is extremely challenging owing to a number of reasons. First, there is a difference in perception about the nature and control of cyberspace domain. According to US, EU and like-minded nations, the internet needs to be free flowing and should be developed and shaped in keeping with market forces, civil society needs, with minimum interference by the government. On the other hand, Russia, China and Iran along with others, consider internet to be an integral domain of the state, which needs to be defended, managed and controlled as per state laws and procedures within the state's territorial boundary. This is also giving rise to the term "Cyber Sovereignty". Second, non availability of common norms and laws provides incentive to a number of state as well as non state players to use the cyberspace domain for carrying out attacks, misinformation campaigns, illegal transactions, crimes etc. with little or no fear of getting caught or facing retribution. Therefore, there is an advantage to be gained by such players if the status of cyberspace domain remains ambiguous and opaque. Lastly, the number of stakeholders affected by the global internet discourse are not only the governments, but also the technological companies, non-governmental organisations, other interest groups and the common people. The concerns of each and every individual, group and state need to be considered while formulating global norms as well as laws.

In spite of being a major stakeholder in the global cyberspace domain, the cyber diplomacy efforts made by India especially for the formulation of global cyberspace norms and laws have been minimal. There has been no major initiative taken by India to drive the global discourse on the nature, use and governance of cyberspace. Though, it has been a member of a number of governmental and non governmental panels and committees but, it has never singly driven any agenda on important issues like cyber laws, cyber governance, accountability and attribution in cyberspace and conduct of defensive and offensive cyber wars, by state as well as non-state actors.

Conclusion

The 21st century has started as a century of uncertainty and unpredictability, change, technology, empowerment of individuals and non-state actors, violence and volatility. For the first time in the history of mankind, we have been able to create, sustain and manage an artificial resource called cyberspace, which can be considered as one of the greatest inventions of mankind akin to the discovery of wheel, printing press, electricity, internal combustion engine and penicillin. While the impact of other great discoveries took time and a lot of resources to reach all the corners of the world; in the case of cyberspace, it was almost instantaneous.

Cyberspace has transformed itself into a major domain like air, land, sea and space. But, unlike other domains which are more or less finite and are equally available to all, cyberspace is being rapidly created and expanded and is not equitably distributed amongst all. Till now, the major responsibility to defend the natural domains of air, land, sea and space rested with the state and its hard and soft instruments of power in terms of defence forces, government and diplomatic corps. Cyberspace, on the other hand, is more or less a privately owned entity with bulk of the ownership being in the hands of mega technological companies which create, manage, police and sustain this ever evolving artificial resource across all natural domains. The states are finding it difficult to, first, manage and defend a domain which is ever growing, is global in nature and being managed by mega corporations. Second, enforcing rules and laws on entities that are geographically independent. Third, they are finding it extremely difficult to replace a global technology or application with a home grown one, due to sheer enormity of technological and financial challenge and lastly, keeping pace with the ever evolving and rapidly changing domain where the major advantage lies with a small number of skilled and nimble individuals and organisations and with the bulky and predominantly outdated instruments of state power.

Cyberspace has turned out to be an extraordinary boon for India. For the first time in the history of the nation, we have witnessed a true leveller which has been able to bridge the divide between the rich and poor and the haves and have nots. This extremely empowering domain has unshackled our dormant innovativeness, knowledge power, business acumen and governance.

Full credit needs to be given to successive governments who early on realised the enormous potential of the cyberspace domain and ensured that the cyberspace infrastructure, especially mobile telephony and OFC backhaul routes were developed at an astonishing pace. The government was also acutely aware that the domain needed to be utilised by the poorest of poor and therefore ensured that mobile and internet services were provided at one of the cheapest rates in the world. It launched a number of ambitious and truly empowering digital programmes like the universal biometric and digital ID Aadhaar, universal health cover, national pension and life insurance schemes.

Presently, India has become one of the most important users and stakeholders in the global cyberspace domain. A major push is being given by the government to provide new age skills and employment opportunities to its youthful population to reap the benefits of the demographic and digital dividend in an aging world. India has been able to attract the largest Foreign Direct Investment (FDI), especially for its technologically driven start ups. Cutting edge research is being carried out in field of AI, robotics, nano technology, quantum computing, blockchain and big data analysis. However, a great deal more is required to be achieved in the shortest possible time. For one, the cyberspace infrastructure is relatively outdated with extremely poor data speeds and OFC penetration. Second, our cyber security posture is relatively inadequate given the large cyber illiterate population, which is extremely susceptible to fraud, fake news and misinformation campaigns. Third, a large number of legislations have not been passed, which makes it difficult to fix accountability and provide assurances to mega corporations looking at India as an investment destination. Fourth, the quality and quantity of cutting edge research which can give rise to transformational industries is lacking, compared to developed nations. Fifth, India has negligible involvement in the global cyberspace industrial ecosystem and is more of a consumer than producer and lastly, there is lack of cohesion and jointness in the sphere of cyberspace as a domain for warfighting.

The appraisal of India's cyberspace ecosystem has been carried out in order to holistically analyse the achievements, limitations and way forward. India, as a nation cannot afford to slacken and slow down the pace of cyberspace development and its exploitation for good governance, commerce, education, health and environment. The coming generations expect it and deserve that from us.

Notes

1. Data from cyber security presentation by Dr V.K. Saraswat, member Niti Aayog at https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf, accessed on October 15, 2019.
2. ITU Statistical report "Measuring the Information Society Report Volume 2, 2018" at https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-2-E.pdf, accessed on October 17, 2019
3. Hootsuite report titled "Digital 2019 Global Digital Yearbook" at https://wearesocial.com/global-digital-report-2019, accessed on October 18, 2019
4. Hootsuite report titled "Digital 2019 India" at https://datareportal.com/reports/digital-2019-india, accessed on October 17, 2019.
5. For full policy document, go to http://dot.gov.in/sites/default/files/EnglishPolicy-NDCP.pdf, accessed on December 23, 2019.
6. TRAI report titled Yearly *Performance Indicator of Indian Telecom Sector 2018* at https://main.trai.gov.in/sites/default/files/PIR_25092019.pdf, accessed on November 12, 2019.
7. Map of data centres in the world at https://www.datacentermap.com/india/, accessed on October 30, 2019.
8. For detailed information, go to http://dot.gov.in/, accessed on October 30, 2019.
9. Draft Personal Data Protection Bill at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf, accessed on January 16, 2019.
10. For further details, go to https://www.cisomag.com/yahoo-data-breach-victims-will-get-us-100-compensation/, accessed on November 3, 2019.
11. MietY Report , "India's Trillion Dollar Digital Opportunity" at https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf, accessed on November 9, 2019.
12. For full project report, go to https://negd.gov.in/sites/default/files/Part1IndEAFrameworkv10Public_0.pdf, accessed on February 11, 2020.
13. Annual report 2018 of CERT-In at https://www.cert-in.org.in/, accessed on November 5, 2019.

14. For complete rules, go to https://meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf, accessed on November 6, 2019.
15. For entire act, go to https://www.congress.gov/bill/116th-congress/house-bill/1158/text, accessed on November 6, 2019.
16. For further details go to https://www.commoncriteria-india.gov.in/node/2, accessed on February 9, 2020.
17. From statistica.com at https://www.statista.com/statistics/268584/worldwide-ict-revenue-since-2005/, accessed on November 8, 2019.
18. Business Standard "Indian ICT revenue to touch US$ 225 billion by 2020: study" at https://www.business-standard.com/article/news-cm/indian-ict-revenue-to-touch-us-225-billion-by-2020-study-118010200212_1.html, accessed on November 9, 2019.
19. https://unctadstat.unctad.org/CountryProfile/GeneralProfile/en-GB/356/index.html, accessed on November 9, 2019.
20. Annual Report 2018-19, Department of Commerce at https://commerce.gov.in/writereaddata/uploadedfile/MOC_637008736055113127_annual_report_2018_19_eng.pdf, accessed on November 9, 2019.
21. National Crime Records Bureau, Mini "Crime in India 2017" at http://ncrb.gov.in/, accessed on November 15, 2019.
22. ET Bureau, "Bengaluru is India's cybercrime capital", *Economic Times* online edition, February 1, 2019 at https://economictimes.indiatimes.com/tech/internet/bengaluru-is-indias-cybercrime-capital/articleshow/67769776.cms?from=mdr, accessed on November 18, 2019.
23. https://cybercrime.gov.in/, accessed on February 20, 2020.
24. All India Survey of Higher Education 2018-19 at https://mhrd.gov.in/sites/upload_files/mhrd/files/statistics-new/AISHE%20Final%20Report%20 2018-19.pdf, accessed on November 19, 2019.
25. Scopus is the largest abstract and citation database of peer-reviewed literature: scientific journals, books and conference proceedings at https://www.scopus.com/home.uri, accessed on November 19, 2019.
26. WIPO Statistical country profile of India at https://www.wipo.int/ipstats/en/statistics/country_profile/profile.jsp?code=IN, accessed on November 19, 2019.
27. WIPO Report titled "World Intellectual Property Indicators 2019" at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2019.pdf, accessed on November 19, 2019.
28. Full report at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, accessed on November 22, 2019.

29. Full report at https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf, accessed on November 22, 2019.
30. Full report at https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf, accessed on November 22, 2019.

6. Recommendations and Conclusion

Information and Communications Technology (ICT) is one of the most potent forces in shaping the twenty-first century. Its revolutionary impact affects the way people live, learn and work and the way government interacts with civil society. IT is fast becoming a vital engine of growth for the world economy. It is also enabling many enterprising individuals, firms and communities, in all parts of the globe, to address economic and social challenges with greater efficiency and imagination. Enormous opportunities are there to be seized and shared by us all.

— Okinawa Charter of the Information Society, 2000

Introduction

We are living in an era of ubiquitous information society. Access to clean, fast and 24x7 internet is essential for personal wellbeing and survival just like food, pure drinking water, clean air and a roof. In fact, a lot of people argue that "Access to Internet" should be considered a fundamental right like the "Right to Education". In Finland, all citizens have a legal right to broadband internet connection with a minimum speed of 1 MBPS, since 2010. Article 7 of the Marco Civil law of Brazil asserts:

The access to the internet is essential to the exercise of citizenship, and the following rights are guaranteed to the users: (a) Non-suspension of the Internet connection, except if due to a debt resulting directly from its use; and (b) Maintenance of the quality of Internet connection contracted before the provider.

We, as world citizens should be immensely proud that we have been able to create an artificial global domain, which has transformed each and every aspect of our lives. It has empowered the weak and oppressed, created immense wealth and opportunity, lifted millions of people out of abject poverty, found cures and remedies for deadly diseases and ailments and crossed new frontiers of science and technology. What is truly remarkable is the fact that we are exponentially creating new ways and means to process, store and transmit information from one entity to another. The domain is expanding and evolving at a rapid pace and connecting millions of new people and devices every second, minute, hour and day.

The internet has also transformed as a global domain which is used for not only information exchange and interconnection but also for crime, misinformation campaigns and warfighting. Use of cyberspace as a domain for warfighting offers immense advantages. First, the instantaneous global reach coupled with extremely low cost of entry. Second, element of surprise, deception, anonymity and non-attributability. Third, ability to cause disproportionate damage and destruction, compared to effort and resources and lastly, the ability to reach out to each and every human to directly influence their hearts and minds.

India is on the cusp of a major digital revolution. There are a number of factors which favour India's transformation into a truly digital empowered nation. First, is the immense faith and optimism that digitisation is the single most important measure to leapfrog development, end corruption, provide good governance, healthcare and education. Second, the numerous initiatives taken by the government for providing pan India internet connectivity at extremely affordable rates. Third, a youthful nation which has readily embraced the digital ecosystem including social media, banking, financial and e-commerce. Fourth, a large untapped market for digital products and services. Fifth, a large English speaking STEM population with a knack for coding, coupled with a large number of science and technology institutes of higher education and lastly, the growing number of cyberspace related start-ups, which are providing innovative products and services at competitive prices.

There are also certain factors which are major impediments to the country's journey towards a truly digital empowered nation. First, a poor cyberspace infrastructure offering one of the world's poorest wireless speeds. Second, relatively poor cyber security posture which results in higher incidents of cyber crime, frauds and incidents of fake news and misinformation campaigns. Third, the relatively lesser spend on R&D, cyberspace technology and innovation. Fourth, an outdated cybersecurity strategy and absence of empowering laws on crucial matters such as data privacy and e-commerce and lastly, a sub optimum system of cyber policy formulation, protection and governance.

The aim of this chapter is to provide certain key recommendations for further improving and optimising the cyberspace ecosystem in India, so that a transformative cyberspace domain is created which is state of the art, secure, clean, affordable and 24x7 available to each and every individual, across the length and breadth of the country.

Recommendations

Vision Statement: To make India a truly digitally empowered nation by 2025.

Goals: In order to make the vision a reality, the following goals are required to be accomplished before 2025:

- Pan India, 24x7, high bandwidth, safe, secure and state of the art cyberspace infrastructure, with a minimum wired speed of 50 MBPS and wireless speeds of 10 MBPS.
- Optimisation of cyberspace governance following the model of "minimum government, maximum governance". Quick and time bound implementation of all government policies, schemes and initiatives. Promulgation and implementation of empowering laws, policies and procedures to create an environment that is conducive for the creation, as well as exploitation of Indian cyberspace.
- Time bound and efficient implementation of cyberspace initiatives and reforms with complete transparency and public participation. Fixing accountability as well as rewarding doers and achievers at all levels of policy formulation and implementation.

- A very high degree of safe and clean pan India cyberspace for individuals, industries, organisations, institutions and government. Defence of cyberspace to be achieved through a system of centralised control with decentralised execution, using world class technology, resources and skill sets.
- Having a vibrant and world class cyberspace based economy (among the world's first five and fastest growing economies) with large number of mega multinational corporations owing entire ecosystems as well as large number of start-ups and digital industrial base of niche cyberspace technologies of AI, robotics, blockchain, big data analytics and quantum computing.
- To become a fully developed cyberspace nation with the lowest incidence of cyber crime and a highly developed and sophisticated anti cyber crime force (among the world's top five).
- Becoming one of the world's top five nations in generating the maximum cyberspace related scientific publications and patents. India to transform into a net importer of cyberspace related high end niche education and skill set with an enviable higher education and R&D ecosystem.
- To acquire the world's best cyber war capabilities that are indigenous, credible, lethal and commensurate with our global and regional aspirations.
- To be at the forefront of international discourse on international cyber laws, norms and standard formulations to ensure a global whole, safe, secure and rule based cyberspace.

Cyberspace Infrastructure

- **Increase mobile subscribers per 100 inhabitants from the existing 87.3 to 100 and active mobile broadband subscribers from the existing 25.8 to 60:** The above can be achieved by promoting manufacturing of mobile phones as well as smartphones within India, like the Samsung phone manufacturing facility in Noida and reducing GST on basic mobile phones, as well as smartphones manufactured inside India.
- **Increasing OFC penetration from the existing 20-25 per cent to 75 per cent by:**

  - Promoting in house manufacturing of OFC cable by giving tax breaks and suitable incentives.
  - Time bound implementation of Bharatnet project for extending broadband connectivity to all Gram Panchayats. Suitable action be undertaken to optimise utilisation and monetisation of entire bandwidth available in the Bharatnet project, to make it commercially viable. The compulsory renting of surplus bandwidth to state, central and other governmental organisations and institutions can be considered.
  - Allocation of 5G spectrum to telecom companies to be linked with captive OFC laid and hired by companies to increase capacity building.
  - Reducing GST slabs on OFC cable and network provisioning equipment.
- **Increasing Data Rates**
  - Minimum wired and wireless broadband data rates be fixed for all telecom service providers to reach minimum data rates of 50 MBPS for wired and 10 MBPS rate for wireless internet services, per subscriber.
  - Providing tax subsidies and incentives for high end telecom network equipment like routers and Dense Wave Division Multiplexers (DWDM).
  - Realistic data access rates per subscriber to improve AGR for telecom companies for making them competitive and viable in the long run.
  - Fast track implementation of pan India 4G and 5G services. Companies from different countries be allowed to compete for fielding next generational wireless networks at the most competitive rates, so that subscriber continues to pay the lowest rates for high speed internet access. Security concerns regarding foreign equipment should be only limited to strategic networks where due precautions can be undertaken.
- **Increase Data Centre capacity from existing 700 MW to 7,000 MW**
  - Leverage the high user base of Indian subscribers of global IT and social media companies like Facebook, Google,

Amazon and Microsoft, to establish tier 3 and tier 4 data centres in India.

- Exploit extremely cold climate of Ladakh as well as parts of J&K, Himachal, UP, Sikkim and North Eastern region to incentivise creation of tier 4 large data centres which are green and require minimum to zero cooling requirements, thereby making them commercially competitive.
- Establish an ecosystem of ICT related industries, enhance skill sets and R&D hubs where special zones are created for niche technologies and major incentives provided for establishing of state of the art ICT infrastructure including data centres.

Cyberspace Governance

- **Centralised Control with Decentralised Execution:** The cyberspace domain is best managed centrally. Thus, it is recommended that Ministry of Communications and MeitY be merged into one Ministry of Cyberspace. This will ensure that all issues pertaining to the domain: like fielding of information infrastructure; allocation of spectrum; policy on tax benefits and incentives to ICT related industries, dealing with internet intermediaries; international representation and positions on various issues, etc. are taken collectively by all the stakeholders and there is unity of intent and resource. Also, it is recommended that the responsibility for defence of cyberspace be given in totality to NTRO, with both ICERT and NCIIPC being under it. A recommended structure of the Ministry of Cyberspace is given at Appendix C.
- **Fast track Promulgation of Important legislations and Policies:** Like Personal Data Protection Bill, National e-commerce policy, National Cyber Security Policy, Intermediary Guidelines Policy, National Encryption Policy, etc.
- **Increase Regional Cooperation in Cyberspace Related Issues:** The BIMSTEC region is a major stakeholder in the global cyberspace ecosystem and accounts for a large subscriber base for almost all social media and other intermediary companies.

There should be a BIMSTEC Cyberspace Forum where collective decisions are taken for formulation of international laws and norms, standardisation, dealing with multinational intermediaries, protection of cyberspace boundaries, storage of personal identifiable information, sharing of data sets for R&D, use of regional operating systems, apps, platforms and banking/ financial tools, etc.

- **Leverage the Indian Cyberspace Ecosystem:** India is a very lucrative and important market for all global internet intermediaries. This should be leveraged to ensure that nation specific improvements are carried out by these intermediaries to ensure that due importance is given to issues of safety, security, social and moral concerns.

Government Initiatives and Digital Reforms: Presently, most of the initiatives and digital reforms are at various stages of planning and execution. The cyberspace domain is an extremely time sensitive domain so it should be ensured that all projects are strictly implemented on time and there is a need to fix accountability and severely penalise concerned individuals, organisations and companies for time slippages. This is because technology gets quickly outdated and any delays can imply outdated technology being used for most of the equipment's life cycle.

Defence of Cyberspace

- **Centralised Control:** Both ICERT and NCIIPC should function under the NTRO and the reasons for the same have been elucidated above.
- **Improvement in Global Cyber Security Index:** A focused approach is necessary for improving the ITU based global cybersecurity index, from present 47 to under 10.
- **Defence of Protected Systems:** It is believed that with the growing digitisation, the number of protected systems need to be increased from the existing four. Also, a greater role needs to be given to NCIIPC with regard to the defence of these systems. All aspects of the network and information storage, access and

analysis, right from inception and fielding through the entire lifecycle needs to be first vetted, cleared and certified by NCIIPC prior to fielding.

- **Creation of a separate CII Audit Agency:** It is proposed that all CII networks and resources should be audited by an autonomous agency that reports directly to Chairman, NTRO. This autonomous agency can be carved out of the existing resources of the ICERT and NCIIPC. Maximum use should be made of PPP model by empanelling certified firms and agencies for auditing of all parts of the network that are not critical or confidential. However, all critical and confidential portions of CII and protected networks should be audited by the skilled manpower of this centralised audit agency, to maintain secrecy and confidentiality.
- **Standardisation:** All procedures, equipment, training and resources employed for fielding, management, security and auditing of critical network be standardised in the same way as US government information systems are standardised by the NIST.
- **Central Procurement:** All equipment, software and applications procured for protected systems needs to be done centrally to ensure optimisation as well as commonality of repair, maintenance and life cycle management of critical systems.
- **International Cooperation:** Further impetus should be given to existing international pacts and Memorandums of Understanding (MoU) on cyber security and information sharing with like minded nations especially in our neighbourhood.

Cyberspace Based Economy

- **Creating of Empowering Ecosystem and Clusters:** There is a need to create domain specialisation clusters of niche technology wherein industry, R&D, educational institutes and skilled workforce co-exist to stimulate innovation and create new generational products and services. For example a blockchain and NLP cluster at Coimbatore; robotics and autonomous vehicle cluster at Bengaluru; Analytics and optimisation cluster at Hyderabad; image recognition cluster at Chennai; annotation cluster at Ahmedabad, etc. These clusters should be suitably incentivised to attract global talent and should have the necessary infrastructure such as reliable electric supply, data centres, high speed internet connectivity, etc. Over a period of time the clusters would acquire a global reputation in their areas of specialisation and spur further growth and innovation in their respective sub domains. In addition, educational institutes and R&D organisations will strive to provide skilled workforce and products which can be easily utilised by the industry to produce products and services at globally competitive rates.

- Develop a universal code of ethics and pass enabling laws for AI technology, blockchain and data sets to provide transparency and clarity to industry and companies willing to invest resource and money into new age technologies.
- Enable and promote regional ICT products, applications and services to help promote Make in India, Make for India and Make for World initiatives, especially in the BIMSTEC region.
- Promote local and regional products, applications and services in government networks and ecosystems.

Cyber Crime

- **Education on Cyber Hygiene, Safe Cyber Practices and Cyber Crime:** There is an urgent need to make education on cyber hygiene, safe cyber practices and cyber-crime compulsory in all schools. In addition, door to door awareness campaigns and education drives need to be carried out regularly, especially in rural areas amongst the first time users of cyberspace.
- **Capacity Buildings:** There is an urgent requirement to open additional cyber police stations in the country along with cyber forensic labs in each state. The initiatives taken by the government in terms of allocation of funds to the states, as well as establishment of CIS division in MHA, I4C and NCFL are praiseworthy, but it is important that the newly created organisations and establishments should have the

requisite capacity in terms of skilled manpower, equipment and applications and function at their optimum capacity.

- **Increase Reporting of Cyber Crime in India:** A large number of cybercrimes especially pertaining to fake news, financial fraud and sexual harassment and molestation go unreported, or do not reach till the justice stage for various reasons. There is therefore a need to ensure hassle free reporting and timely disposal of all cybercrimes occurring in the country. Establishing of a National Cyber crime reporting portal[1] is a step in the right direction.

Cyberspace Related Skillset and Workforce

- **Become Preferred Destination for Higher Education for Foreign Students:** It is observed that of the total 37.4 million students enrolled for higher education in India, only 47,427 are foreign students. India has one of the best systems of higher education at very competitive cost. However, we have been unable to attract foreign students who will not only contribute towards the national economy but would greatly enhance the quality of research being carried out in our colleges and universities, especially in fields related to cyberspace technology.
- **Improve Quality and Quantity of International Publications and Patents:** The SCImago journal and country rankings indicate that though India features among the top 10 countries with regard to internationally citable publications, countries like UK, Germany, Japan, Canada and France are ranked higher than India in spite of having fewer students and research institutes. Thus, it is imperative that India should improve the quality as well as quantity of research and its ranking to appear among the first five countries globally, especially in STEM fields.
- **Provide Industry Specific Skillset to Students:** As stated earlier, there is a need to establish domain specialised ecosystems or clusters at specified locations that can make a reputation for themselves in their areas of specialisation. In line with this, it is recommended that higher educational as well as R&D institutes in the vicinity of these ecosystems or clusters, should provide skilled graduates who can be employed by the industry.

- **Improve and Increase R&D Efforts of Institutes of Higher Education:** The rise in the numbers of patents filed by India in the last five years with a YoY growth of 27.2 per cent is worthy of appreciation. It is recommended that more incentives be offered to our R&D organisations and institutions, so that India can feature among the top 10 patent filing countries by 2025.
- **Improve Global rankings of Indian Universities and Institutes, especially those in STEM Fields:** The Times Higher Education Global rankings 2020 included six India institutes among the world top 500 institutes with Indian Institute of Science, Bangalore topping the Indian institutes, with a world ranking of 301 out of 350. There was no Indian institute in the first 300 institutes. There is thus a need to improve our global ranking which greatly depends on the quality of research, faculty, infrastructure and funding. It is recommended that the government funding to institutes be regulated on basis of parameters ranging from quantity and quality of international publications, patents filed and global institutional rankings.

Cyber Laws: Cyberspace as a domain is generally referred to as the “Wild Wild West” owing to the very high degree of anonymity and attributability, as well as absence of international laws and norms. A safe and secure cyberspace is essential for a fast developing country like India. Due to the fast changing nature of the domain, it is essential that legislations dealing with cyberspace are revisited at periodic intervals and amended from time to time. The IT Act was last amended in 2008 and thus needs to be revised to ensure that the legislation remains relevant today. In addition, there is a requirement to fast track a large number of pending legislations and policies like the Data Protection Law, Draft Intermediaries Guidelines Rules 2018 and Draft National e-Commerce Policy.

There is also an urgent necessity to formulate international cyber laws, especially those pertaining to the norms and use of cyberspace dimension, as part of a nation’s hard and soft power matrix in order to ensure a safe, secure and rule based cyberspace.

It is important that India takes a lead role in formulating critical international cyberspace legislations, as it is a major stakeholder in the global cyberspace ecosystem. India is not only a key contributor of cyberspace related products, services and technologies but also has the highest subscriber base of a large number of social media and other new age applications and platforms.

Cyber War, Deterrence Capacity and Capability

- Full operationalisation of the DCA at the earliest.
- Merger of all Service specific cyber groups/agencies under the DCA.
- Creation of a cybersecurity R&D agency under DCA, with primary staffing from DRDO.
- Establishing a pan India cyberspace common for all the three services and other organisations of MoD.
- Creation of an independent cyber audit agency which functions and reports directly to the CDS.
- Clearly defining the role, charter and responsibilities of each service and organisation fielding, maintaining and utilising cyberspace. Clear demarcation of roles, tasks and responsibilities of persons in uniform and those who are not (defence contractors, other government agencies, etc.), need to be clearly enunciated and defined.
- Formulating cyberspace doctrines, procedures and protocols.
- Establishing common standards of equipment, applications, operating systems and personnel used for establishing, maintaining and auditing the defence cyberspace and cloud.
- Standardisation and formulation of common audit and emergency response task force protocols and procedures.
- Joint training, capacity building and skill building of strategic assets and resources.
- Common procurement of all ICT equipment, applications and services for the three services and other organisations of MoD.

There is also a requirement to clearly enunciate the cyberspace doctrine of warfighting, as it provides a strategic road map to the defence forces for preparation, capacity and capability building, as well as informs the general public, researchers and international community about the broad contours of the nation's resolve towards use of cyberspace, as a domain for warfighting.

Cyber Diplomacy: It is strongly recommended that India should play a leading role in driving the international community's agenda for formulating global cyberspace norms and legislation. There are a number of reasons for this. First, India is a major stakeholder in the global cyberspace ecosystem. Though China may have more users connected to the internet but, the internet in China is far different from the free and open internet available across the globe. Also, China is not a major stakeholder in multinational social media companies like Facebook and Google. Second, lack of norms creates an environment of uncertainty, opacity and criminality. As more and more people, organisations/ institutions and devices join the global cyberspace and it becomes a basic necessity for survival like water and air, we can ill afford to live in an uncertain, polluted and crime prone cyberspace domain. Third, the cyberspace domain is being weaponised at a rapid pace. This can reach a stage wherein, countries that are unable to keep pace with the strategic technological advantage of a cyber weaponised state might have to succumb to pressures and dictates of these states, which would again lead to a global divide into countries that possess strategic cyber weapons and those that do not. Thus, it is in the best interests of India to take the lead and project itself at the fore front of global initiative for cyber norms creation and formulation of international cyber laws.

It is also important that India enters into all-encompassing strategic cyberspace treaties with a large number of countries, especially those in the immediate neighbourhood, as well as those such as USA, China, Russia, Japan, UK, Australia, Israel and France who also have major stakes in the global cyberspace domain. India also needs to emerge as a champion country which strongly opposes weaponisation of cyberspace and should propagate the use of cyberspace for the greater good of humanity and the environment.

Conclusion

The Instantaneous Age: We are presently living in the *Instantaneous* age. The transition from *Information* age to *Instantaneous* age took place during the first few years of the 21st century. The *Instantaneous* age is characterised by a number of tectonic shifts, each making the age more unique, unknown and unprecedented compared to the previous known ages of hunter gatherer – agriculture – industrial and information. First, the scale of progress and change has transformed from linear to exponential and logarithmic. A cursory study of emergence of new technologies and businesses in the last decade or so, will more than prove this statement. Second, wealth generation by utilising natural resources like the manufacture and supply of oil and minerals, has more or less stagnated. Real wealth generation is being achieved by monetising artificial resources like data and intelligence. Third, there has been a shift in a nation's power centre. Earlier, the power centre of a state was its leadership and government. Presently, mega corporations and private enterprise which have a global presence and generate enormous wealth and intellectual capital are the new centres of gravity of a state. Fourth, ideas and intellectual property are the most critical capital and resource of a state. Major breakthroughs in AI technology have proved time and again that the code or algorithm is more powerful than the machine. A $35, Rasberry Pi based AI system, developed by a doctoral student of the University of Cincinnati was able to defeat a US Air Force trained pilot in combat simulation in June 2016.[2] Fifth, easily available off the shelf technology and equipment, can empower individuals and weak organisations to target and cause harm to major states and organisations. The attack by Houthi rebels that successfully targeted and destroyed oil processing facility at Abquaiq and Khurais in Saudi Arabia on September 14, 2019 is an example of this type of strategic empowerment at low cost. Lastly, the instantaneous age is giving rise to a new global world order where mega corporation are creating enormous wealth and causing disruptions and paradigm shifts in previous age based industry and employment bases across the globe. The wealth which was earlier being generated in decades is now being generated in years and months by neo age mega corporations founded in a short time span by new age tech gurus and innovators, most of whom are teenagers or in early twenties.

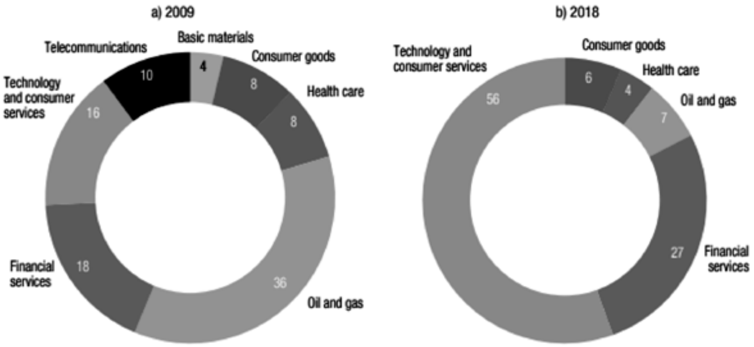
These mega corporations wield enormous power, overcome and stifle competition, own the entire ecosystem and pick flags. There is an all pervasive culture of winner takes all. Nation states who have a large number of these IP and niche technology based mega corporations, in turn wield enormous influence and prosper. On the other hand the states who are serviced by these mega corporations reap the benefits of digital empowerment at low capital cost but lose out on indigenous technological advancement, flight of home grown and in house generated data and more or less become entirely dependent and at the mercy of the digital ecosystem created by these mega corporations.

United Nations Conference on Trade and Development (UNCTAD) in their "Digital Economy Report 2019"[3] has highlighted this tectonic shift in wealth creation in the 21st century. It states:

Digital advances have generated enormous wealth in record time, but that wealth has been concentrated around a small number of individuals, companies and countries. Under current policies and regulations, this trajectory is likely to continue, further contributing to rising inequality.[4]

A comparison of the market capitalisation of world's top 20 companies in 2009 and 2018 adequately proves the above statement. In 2009, the top 20 companies in the world comprised of seven companies in the oil and gas and mining sector, three companies in technology and consumer services sector and three companies in the financial sector. In 2018, it was eight companies from the technology and consumer services sector, seven from the financial sector and only two from the oil and gas and mining sector. What is more surprising is that four of the top ten companies in 2018, namely Amazon, Alibaba, Facebook and Tencent, did not feature in the top 100 companies in 2008.

Figure I.16. World's top 20 companies by market capitalization, by sector, 2009 versus 2018
(Per cent)



Source: UNCTAD, based on PwC, 2018b.

Among the world's 70 highest valued digital platforms, most are based in USA followed by China. US digital companies have a 70 per cent market capitalisation share of the world in this sector with the US hosting more than half of the world's top 100 websites.

The Age of Mega Corporation: The new age mega corporations need a very specific and niche ecosystem to create and sustain them. Herein also lies their vulnerability. Some of the key ingredients are given in succeeding paragraphs.

Peace, stability and rule of law are the most essential ingredients for setting up and sustaining a mega corporation. High end niche human skill sets are the most important assets of these new age industries. Such a skill set will never be available in any one region or part of the globe and needs to be suitably incentivised and motivated to relocate from different parts of the world and become part of the newly raised company.

Second, high end digital infrastructure in terms of power, storage, data sets and computational resource with high speed internet access is a key necessity. Third, a thriving knowledge ecosystem with a large number of English speaking STEM graduates and research and development institutions within a geographical area add immense value to new mega corporations. Fourth, funding which was a major requirement in earlier years, is no longer an issue due to the large number of venture capitalists and angel investors looking to grab a piece of the pie in the formative years. Fifth, governmental incentives in terms of tax breaks, custom duty exemptions, corporation friendly policies, lenient bankruptcy laws and ease of doing business, go a long way towards the fast scaling up of the company, as well as for increasing the risk taking appetite of the mega corporation.

Lastly, once a mega corporation is locally well established and has been able to carve out a niche space for its products and services in the hugely competitive global market, there is a need for the government to promote global standards, policies and laws which best serve the mega corporation's interests as well as its intellectual property. Then only will the mega corporation really fulfil its global ambitions and start creating an exclusive ecosystem which results in massive wealth generation and strategic leverage.

Since a mega corporation requires a very specific type of ecosystem to sustain and generate wealth, a disruption in a part or whole of this ecosystem will result in the mega corporation greatly losing out on its wealth creation and strategic leverage.

First, disruption of peace and stability in the country where a mega corporation is based will lead to the flight of skilled manpower as well as capital. Second, mega corporations are exceedingly vulnerable to new technology, that completely and suddenly overthrows existing technologies, revenue generation models and practices. Introduction of taxi aggregator services like Uber and Ola and their effect on local taxi businesses is an example of the above. Third, infringement of intellectual property and copying/stealing of proprietary technology or knowledge will result in the mega corporation losing out on its major leverage to generate clientele and wealth. Fourth, restrictive trade barriers, local laws and policies enforced by countries which host the major clients or generate maximum revenues, will also greatly affect the corporation in the long run. Fifth, change in global standards, laws and trade practices which directly impact the business and revenue models of mega corporations. Sixth, fragmenting the global supply chains and processes and lastly, initiating investigations, lawsuits and imposing substantial fines/penalties on leadership and mega corporations also add to the list of vulnerabilities.

Conflicts in the instantaneous age will be constant, hybrid, cross domain and interspersed with moments of extreme violence, followed by periods of relative peace, calm and tranquillity. These never ending conflicts will tire out individuals and nations, create islands of peace, wealth and prosperity around oceans of depravity and violence. If a country is able to create a mega corporation which is capable of giving reasonable competition to an adversary's mega corporation in similar fields then, the winner between the battle of corporations will eventually decide on the net leverage enjoyed by a particular country in the global arena, of niche technology.

India in the Instantaneous Age: In such a high stakes competitive space where a considerable lead has been taken by the US, China as well as other technology savvy countries like Japan and UK, the alternatives available to India and the role of defence services in the overall game plan, remains the moot question which needs to be deliberated and answered.

First, the primary objective for India is to garner space and elbow room for itself in this exclusive club dominated by the US and China. Thus, a whole of nation approach is critical for India to catch up. The whole of nation's approach however, can only work when the vision, goals and objectives are clearly defined, demarcated and monitored at each and every step.

Second, the market size, scale of data generation, demography dividend, large English speaking STEM population and growing aspirations and the GDP of the nation, needs to be leveraged to generate traction and increase share of involvement in the global digital ecosystem.

Third, India needs to create a large number of mega corporations in niche technological areas of AI, block chain, robotics and big data analytics in order to reap the digital dividend of the next generational, deep impact technologies. These mega corporations can only be created if the right ecosystem, as elucidated above, is created for them to thrive and create space in the global marketplace. One major factor in our favour is that next generational technologies use the algorithm or code along with vast quantities of data sets, as the primary resource for creating products and services. The availability of skilled manpower as well as a large volume of data available with us, needs to be optimally exploited.

Fourth, India is situated in the middle of the world's most violent zone and is facing threats and challenges to its peace and security. The challenges range from nuclear showmanship to conventional conflict, cross border terrorism, left wing extremism, maritime security and piracy. A peaceful and rule based environment is essential for creating and sustaining the mega corporation. Herein lies the challenge for our defence forces.

Fifth, in spite of rapid progress made in the last couple of years, India still has a comparatively poor digital infrastructure, power grid and cyber security posture. The same needs to be fast tracked.

Sixth, we need to create indigenous technologies and products for consumption within India, as well as become the number one choice for ICT products and services in the neighbourhood, especially within the BIMSTEC region, in order to become a major regional player.

Lastly, there is a need to play a more proactive role in international forums, especially those pertaining to standards and global norms, laws and policies in the cyberspace dimension.

An attempt has been made to give the reader a broad overview of the extremely complex and fast changing cyberspace domain. This artificial domain is one of the most defining achievements of the human race and is capable of propelling us into the future at a pace which has never been witnessed before. For the professional dealing with the innumerable facets of this domain, this book is meant to offer an insight and knowledge which would hopefully assist in formulating policy and decision making. For the layman, the book provides the big picture and a glimpse of things to come.

Notes

1. https://cybercrime.gov.in/, accessed on February 11, 2020.

2. Cuthbertson, Anthony. "Raspberry pi-powered AI beats human pilot in dogfight", *Newsweek*, June 28, 2016 at https://www.newsweek.com/artificial-intelligence-raspberry-pi-pilot-ai-475291, accessed on July 13, 2019.
3. UNCTAD, "Digital Economy Report 2019" at https://unctad.org/en/PublicationsLibrary/der2019_en.pdf, accessed on October 25, 2019.
4. Ibid., p. iv.

Appendix A

CYBERSPACE ARCHITECTURE AND BUILDING BLOCKS

1. **Network Models:** There are two basic models on which the entire cyberspace networks are built:
   (a) **The Open Source Interconnection (OSI) Model:** The OSI model was jointly developed by the International Organisation for Standardisation (ISO) and International Telegraph & Telephone Consultative Committee (CCITT in French, presently Telecommunication Standardisation Sector of International Telecommunication Union (ITU-T)) and published in 1984 as Standard ISO 7498 and X.200 of ITU-T.

   The OSI model divides a networking system into seven *layers*. The functionalities of each layer are implemented by one or more *entities*. Each entity interacts directly with the layer immediately below it and provides functionalities for use to the layer above it. Host entities of a particular layer interact with their counterpart entities of same layer in different host by use of *protocols*.

Layers of OSI Model

	Layers	**Protocol Data Unit (PDU)**	**Function**	**Example Protocols**
Host layers	7. Application	Data	High Level Application Programming Interface (API), including resource sharing, remote file access	HTTP, FTP, SNMP, Telnet
	6. Presentation	Data	Data translation between network services and application	SSL, TLS

	5. Session	Data	Managing communication sessions between hosts	Net BIOS, PPTP
	4. Transport	Segment, Datagram	Transmission of data segments between points in a network including segmentation, multiplexing and acknowledgement	TCP, UDP
Media Layers	3. Network	Packet	Addressing, routing and traffic control	IP, ARP, ICMP, IP Sec
	2. Data Link	Frame	Transmission of data frames between two nodes connected by physical medium	PPP, ATM, Ethernet
	1. Physical	Bits	Transmission and reception of raw bit streams over a physical medium	Ethernet, USB, Bluetooth, IEEE 802.11

Data processing between two nodes is done as under:

(i) Data to be transmitted is composed at the topmost layer (layer N) into a Protocol Data Unit (PDU).

(ii) This PDU is sent to the immediate lower layer (layer N-1) where it is called a Service Data Unit (SDU). This SDU is given a header and/or footer and thereafter becomes the PDU of layer N-1.

(iii) This PDU is sent to the next lower layer (Layer N-2) where the process is repeated.

(iv) At layer 1 bits are transmitted from the transmitting Node to the receiving Node.

(v) At the receiver, the PDU flows from lowest layer to the highest layer where the headers and/or footers are stripped at each higher layer and data processed and thereafter passed on to the next higher layer.[1]

(b) **The Transmission Control Protocol/Internet Protocol (TCP/IP) Model:** The TCP/IP model was designed and developed by the US DOD and was first published in 1974. In March 1980, the US DOD declared it as a standard for all US military communication systems.[2]

The TCP/IP model consists of four layers, but the layers are not rigid in their implementation like the OSI model. The four layers are *Application, Transport, Internet* and *Link*. Details of the same are given below.

(i) **Application Layer:** The application layer consists of a set of protocols for providing user services or exchanging application data over the network connections established by lower level protocols. Examples of application layer protocols are Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Dynamic Host Configuration Protocol (DHCP).

Data coded according to Application Layer protocols are encapsulated into Transport layer protocol units (like TCP or User Datagram Protocol (UDP)) which in turn use lower layer protocols to affect actual data transfer.

Unlike OSI model, the TCP/IP model does not define additional layers between Application and Transport layer (Presentation and Session layers of OSI model). The TCP/IP model distinguishes between the user protocols and the support protocols. The user protocols are used by a particular application while the support protocols are essential for the functioning of the networking system.

(ii) **Transport Layer:** This layer establishes host to host connectivity over the network and protocols in this layer provide error control, segmentation, flow control and application addressing (port numbering).

For the purpose of providing process specific transmission channels for different applications, the transport layer has a concept of network ports. For different services the logical port numbers have been standardised so that client computers may address specific services of a server computer without using service announcements or directory services.

TCP is a connection oriented service while UDP is a connection less services. Both the protocols are '*Best of Effort*' delivery protocols.

(iii) **Internet layer:** This layer is responsible for sending packets of data over multiple networks. The internet layer performs two basic functions:

(aa) **Host addressing and_identification:** By using Internet Protocol (IP) addressing scheme.

(ab) **Packet Routing:** Sending packets of data (datagrams) from source to destination by forwarding them to next network router closest to final destination.

The layer provides unreliable datagram transmission facility between hosts located on different IP networks. The IP is the basic protocol of the Internet layer. The original addressing system of the ARPANet and its successor, the internet was the Internet Protocol Version 4 (IPv4) addressing system. It was a 32 bit addressing system that could identify approximately four billion hosts. This limitation was removed in 1998 by standardisation of IPversion6(IPv6) which uses 128 bit addresses.

(iv) **Link Layer:** It is the lowest component layer of the TCP/IP model as the model is designed to be hardware independent.

The Link layer is designed to move packets between the Internet layer interfaces of two different hosts on the same link. The process of transmitting and receiving packets on a given link can be implemented by using software device drivers in the network card or as a firmware on specific chipsets.

The Link layer performs Data Link layer functions like adding the packet header and transmission of frames over the physical layer. The TCP/IP model includes specification of translating the networking addressing methods used in the IP to Link layer addresses, such as Media Access Control (MAC) addresses.

2. **Types of Networks:** Depending on the geographical spread, number of users and usage, networks are generally classified as under:

(a) **Personal Area Network (PAN):** A PAN, as the name suggests is a network created and administered by a single individual for personal use in small offices or residence. It usually consists of a single internet connection terminated on a hybrid switch providing both cable as well as Wi-Fi access to which two to three computers, mobile phones, printers etc are connected.

(b) **Local Area Network (LAN):** The LAN is one of the most widely used computer network. It covers a small geographical area (a building or number of buildings) and connects a number of computers and networking devices. The LAN generally connects to other LANs or other larger networks using a router. LANs are administered by LAN administrators, who generally perform network management functions like granting access rights and other network housekeeping functions.

(c) **Campus Area Network (CAN):** These are usually larger than LANs and cover a bigger area than LAN like universities, schools, companies, etc. The network generally connects a group of buildings of a single organisation/ institution.

(d) **Metropolitan Area Network (MAN):** It covers a larger geographical area than a LAN or CAN, usually the size of a city or a town. A MAN is typically managed by different telecommunication companies or Internet Service Providers (ISPs).

(e) **Wide Area Network (WAN):** These interconnect larger geographical areas like different cities separated over large distances. High capacity bulk media is used for data transfer between the different cities and towns. The inter city/town connectivity is referred to as *backbone* connectivity while the connectivity within a particular city of town is referred to as *access* connectivity. The internet is the largest WAN.

(f) **Storage Area Network (SAN):** These are dedicated high speed networks that connect different servers to a common pool of storage devices, generally kept at different geographical location. These do away with data being stored by individual users on their machines and provide similar functionality with additional advantages of better data protection, management and redundancy.

(g) **Enterprise Network:** An enterprise network is an exclusive network established by a large organisation to interconnect various IT resources of that organisation over different geographically separated areas. An enterprise network is costly, takes comparatively larger time to create but being exclusive can provide better performance, security, redundancy and resilience.

(h) **Virtual Private Network (VPN):** The VPN mimics an exclusive network between different geographical locations of an organisation over the internet. The advantages of a VPN over an exclusive network is that it takes considerably lesser time, cost and resources to set up and provides almost similar levels of security and performance.

(i) **Cloud Networking:** Provisioning of networking resources by a third party over the internet is referred to as *cloud*. *Cloud* computing and network sharing has become very popular lately due to availability of cheap and stable internet access with high data rates.

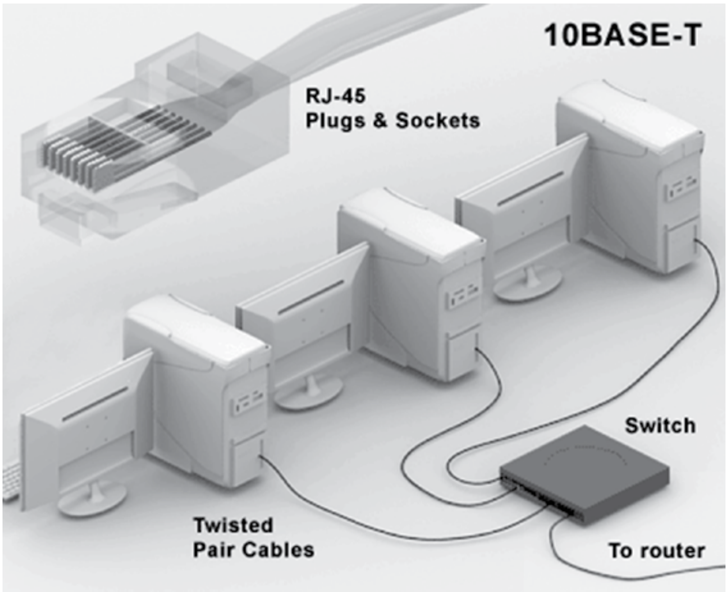
3. **Basic Hardware Building Blocks of a Network:** At the hardware level, networking is firstly established between the end user devices (personal computer (PC), mobile, printer, network storage devices, etc.) and the PAN/ LAN, secondly within the LAN and subsequently multiple LANs

interconnect within the WAN to give rise to the internet or an exclusive enterprise network.

The various hardware devices/technologies used in creating the network are as under:

(a) **Interconnect between the end user device and PAN/LAN**: Depending on the type of end user device (PC/mobile/printer/storage device, etc.), both wired and wireless connectivity to the PAN/LAN is possible. These are :

(i) **Ethernet (10/100 Base T):** This is a wired standard known for transmission at 10 Mega Bits Per Second (MBPS)/100 MBPS. Introduced in 1995, it is the IEEE 802.3u standard. Most of the computer network cards connect to the switch or hub using the Registered Jack (RJ 45) connector and Unshielded Twisted Pair (UTP) cable using this standard.



Source: pcmag.com.

(ii) **Blue Tooth**: It is a wireless technology standard (IEEE 802.15.1) for exchanging data over short distance (typically less than 10 meters) using the Ultra High Frequency (UHF) Industrial Scientific & Medical (ISM) band from 2.4 to 2.485 GHz for connectivity in PANs.

(iii) **WiFi or Wi-Fi**: It is a technology for radio wireless networking of devices using the IEEE 802.11 standard. Devices connect to the internet or PAN/LAN using a Wireless Access Point. The Wi-Fi standard uses the 2.4 GHz UHF or 5.8 GHz Super High frequency (SHF) ISM band for transmission and reception. These are *line of sight* frequencies and can be easily absorbed by certain materials like concrete, etc.

(b) **Interconnection between LAN/MAN/WAN:** Interconnection between various LANs and WANs are created by using either hubs, switches or routers. Details of the same are given as under:

(i) **Ethernet Hub:** These are the cheapest and simplest devices to interconnect multiple computers and IT devices in the network. The Ethernet hub uses only Ethernet cable and RJ45 connector to connect the port of Network Interface Card (NIC) of computer with the hub. Each hub has a number of ports (generally 4 to 5) for connecting various computers and IT devices (one port to each device). Expansion of the network can be done by connecting an Ethernet hub to other hubs or switches or routers. A hub operates only at layer 1 of the OSI model and is poor in network security features.

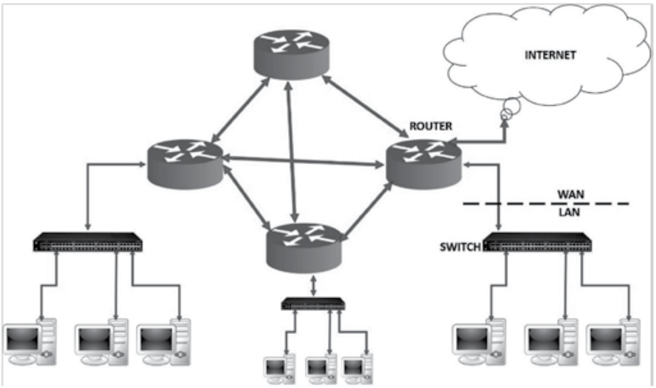
(ii) **Network Switch**: A network switch is similar to a hub in the sense that it also uses wired media (ethernet cable or fiber optic cable) for interconnecting various IT devices and providing network access. However, unlike a hub which operates only at layer 1 (physical layer) of the OSI model, the switch is more intelligent and operates either at layer 2 (Data Link Layer) or layer 3 (Network layer) of the OSI model. The network switch is capable of segmenting various ports into different collision domains in order to have collision free transmission and reception of data packets. In addition, high end switches (called multi layer switches) are capable of configuring each and every port to ensure optimum performance and advanced security features over the network.

Source: Wikipedia.

(iii) **Router:** It is the most crucial equipment of a WAN and is used to interconnect different LANs, by following different protocols seamlessly. The internet can be described as a network of routers with multiple LANs connected to each router.

Routers are responsible to first determine that the destination address of data packets belong to the same network or to a different network. This it does by accessing a dynamic routing table which it continuously builds and updates by exchanging information with other routers, connected to the network. Thereafter the router encapsulates the data packet with routing protocol header and sends the data packet to the next router for further transmission till the destination machine.

In addition, the routers perform additional functions of calculating the shortest path to a particular node, error correction, collision detection and encryption.



(c) **Networking Media:** The interconnection between various networks can broadly be classified into *access media* (interconnection at LAN and PAN level) and *backbone media* (interconnection at WAN level). Details of the same are given below:

(i) **Access Media**: It can be either wireless (Wi-Fi) or wired (cat 5/cat 6 UTP cable or OFC). Since OFC is largely used for backbone media connectivity, its details will be covered subsequently.

Cat5 and Cat 6 UTP cables are two different types of twisted copper cables for interconnection at the LAN level. The cables are twisted in order to reduce electromagnetic interference. The cat 5 cable consists of two pairs of twisted copper wires and provides a range of 100 meters with data speed of 100 MBPS. The cat 6 cable consists of four pairs of twisted copper wires and provides a range of 100 meters with a data speed of 1 Giga Bit Per Second (GBPS) or 50 meters with a data speed of 10 GBPS.

(ii) **Backbone Media:** The backbone media can also be wireless (Satellite, Microwave or Wi Max) or wired (OFC).

(aa) **Satellite:** Satellite communications are used for providing connectivity in far flung areas and as a backup to terrestrial media. Communication satellites are launched into one of the three orbits. The Geostationary orbit which is roughly 36,000 km above sea level with the satellite's orbital period being the same as the rotational rate of earth. The satellite appears to be stationary over a fixed point and does not require ground station antenna to continuously track it. A constellation of three satellites in Geostationary orbit can roughly provide connectivity to the entire globe. The Medium Earth Orbit whose orbital altitude varies from 2000 km to 36,000 km and the Low Earth Orbit (LEO) whose orbital altitude varies between 160 km to 2000 km. Because of their proximity to Earth, the LEO satellites are relatively cheaper to launch and provide higher Signal to Noise Ratio (SNR). However, the satellites are visible over a radius of roughly 1000 km and therefore require a large number (66) to provide uninterrupted global connectivity.

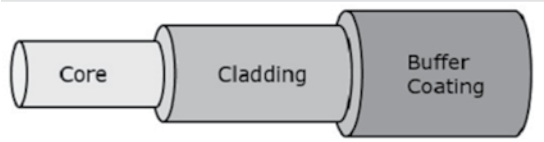
The communication payload of a communication satellite consists of transponders, antennas and switching equipment. Frequency assignment of satellite systems is accorded by the ITU. Modern communication satellites are capable of offering data rates as high as 506 MBPS[3].

(ab) **Microwave**: The microwave frequency band covers the range from 300 Mhz to 300 GHz of the electromagnetic spectrum. The microwave communication systems are line of sight (range of one Link is approximately 40 km) and are much preferred due to their smaller antenna size, narrow beam width and higher data rates. The range of microwave systems can be extended substantially by having a chain of repeater stations between two communication nodes.

(ac) **WiMAX**: The WiMAX technology is a broadband data communication technology based on IEEE 802.16 standard and is used to provide high speed broadband wireless access for both mobile as well as fixed applications for MANs. The letters WiMAX stand for Worldwide Interoperability for Microwave Access. WiMax uses Orthogonal Frequency Division Multiplexing (OFDM) and Multiple Input Multiple Output (MIMO) technology to provide higher data rates (up to 15 MBPS) and better throughput.

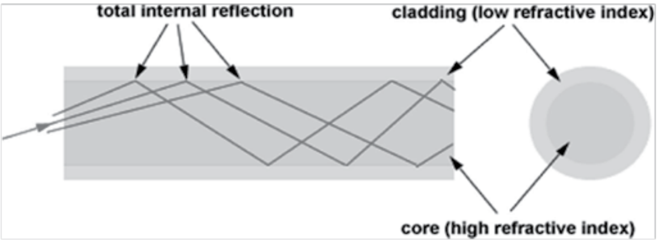
(ad) **OFC:**[4] Optical Fibre Cables are long thin strands of very pure glass about the diameter of a human hair. They work on the principle of total internal reflection.

The optical cables are composed of core, cladding and buffer coating. The core is the inner part of the cable which guides the light. The refractive index of core is kept higher than that of the cladding to ensure that light travelling along the core gets totally reflected back into the core with no spill over in the cladding (Total internal reflection). The buffer coating provides mechanical protection and bending flexibility to the fibre. The light source is either Light Amplification by Simulated Emission of Radiation (LASER) or Light Emitting Diode (LED).



Parts of an Optical fiber

Source: www.tutorialspoint.com.


total internal reflection
cladding (low refractive index)
core (high refractive index)

Source: www.fiberoptics4sale.com.

A fibre optic cable can be single mode (fibre diameter of 8.3 to 10 micron, only one mode of transmission, higher data rate and up to 50 times more distance as compared to multi-mode fibre, light source is LASER) or multi-mode (fibre diameter 50 to 100 micron, multiple modes of transmission, lesser distance and data rates, light source is LED)

The OFC is the preferred media for backbone communications because it offers high data rates, less power loss, longer range, immunity to electromagnetic interference (EMI), higher security, immunity to electrical noise, less weight and size as compared to copper cable, cheaper, durable and long lasting.

Using advanced multiplexing technologies such as DWDM, data rates of up to 100 Giga Bits Per Second (GBPS) are possible per channel with each pair of fibre optic cable capable of transmitting and receiving up to 80 channels simultaneously.

4. **Mobile Communications:** The mobile communication system typically consists of last mile connectivity between the mobile phone and host *Base Station* on wireless media. The basic system consists of hexagonal cells with each cell being serviced by a Base Trans-receiver System (BTS or *Base Station*) and multiple *Base Stations* getting connected to a *Mobile Switching Centre* (MSC). The *Base Stations* continuously transmit a beacon frequency for mobiles to determine the nearest *Base Station* in order to hook on to it. When mobiles move between one *Base Station* and another, a *handoff* takes place between the mobile and both the *Base Stations*. This *handoff* can be hard (break before make) or soft (make before break). Bulk of the call drops occur during *handoffs*.

Mobile Communication Standards: The basic challenge for all mobile service providers is to offer highest data rates to maximum users within a fixed EM spectrum. The same is achieved by applying one or a combination of two or more multiplexing techniques viz Frequency Division Multiplexing Access (FDMA), Time Division Multiplexing Access (TDMA), Code Division Multiplexing Access (CDMA) or Orthogonal Frequency Division Multiplexing Access (OFDMA). A comparison between various generations of mobile technology with services and maximum data rates is given as under:

GENERATION	SERVICE	MAXIMUM DATA RATE	STANDARD
1g	Voice only	2.4 Kbps	AMPS
2g	SMS & MMS	64 Kbps	GSM, IS-95
3g	Data, video & mobile internet	2 MBPS	WCDMA, CDMA 2000, UMTS
4g	High Speed data	100 MBPS-1Gbps	WiMax, LTE
5g	Not yet fielded	Up to 20 Gbps	Millimetric wave communications, massive MIMO

5G Mobile Communications: The latest standard in mobile communications is the 5G which is all set to revolutionise the way information is stored, analysed and applied in the cyberspace with a host of novel technologies like autonomous vehicles, immersive games and tele medicine banking heavily on it.

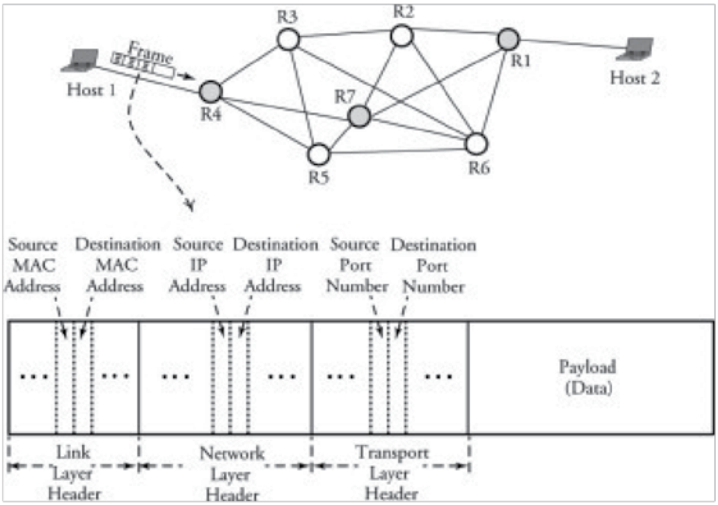
The fielding of autonomous vehicles on the road, requires high bandwidth and a reliable wireless network which can be provided by 5G networks. In addition, with the coming of IoT, the number of devices being connected to the internet will increase exponentially. 5G networks promise a download speeds ranging from a few GBPS to 20 GBPS. Three major categories of use have been identified for 5G. These are: massive machine to machine communications for IoT; ultra-reliable low latency communications for mission critical devices; autonomous vehicles; industrial robots; safety and disaster management systems, etc.; and enhanced mobile broadband for a faster and richer experience for a host of applications. The reason why 5G is able to provide continuous connection with high bandwidth and faster response times is due to: firstly, small cell size which ranges from 10 metres to a few hundred metres so that a large number of wireless devices can be connected to the base station. Secondly, higher spectrum range for working i.e. 600-700 MHz, 3-4 GHz, 26-28 GHz and 38-42 GHz. The higher spectrum range provides a higher bandwidth per device and is capable of providing high speed connectivity to multiple devices. Thirdly, use of Massive MIMO antennas by both the end device as well as the base station. The antenna size of 5G systems is small because of the higher frequency. Multiple antennas are mounted at the device and base station end and multiple signals are received at the end device from multiple base stations and using the techniques of beam steering and beam forming, it is ensured that signals from the Base station to the end user device are directed and synchronised resulting in a high throughput. Lastly, high latency (faster response time) is achieved by use of better technology and network architecture.

5. **Addressing Schemes:**[5] This is a very important aspect of any network, especially internet. It enables the network to determine the originator as well as source of data packets. The second, third and fourth layers (transport, network and Link) of TCP/IP model produce a header which is essential to determine the routing of data packets from the source to the destination:

(a) **Link Layer Header**: It consists of 6 bytes (48 bits) and called the MAC address and is represented as a six field hexadecimal number like 89-A1-33-2B-C3-84. Each hardware interface to the network has its own MAC address (each Network Interface Card on every PC/laptop/mobile/tablet in the world will have its own unique MAC address). A Link layer address contains the MAC address of both the source as well as destination interfaces.

(b) **Network Layer Header**: It is 4 bytes long (32 bits) and called IP address. It is represented by four fields, each of one byte length separated by a dot e.g. 192.2.32.83. Each entity in the network must have an IP address. A network layer header contains the IP addresses of both the source as well as destination IP addresses.

(c) **Transport Layer Header**: It is 2 bytes (16 bits) long and identified by a port number (like port number 3454). A networking device can be running a number of networking applications simultaneously. Therefore, there is a need to identify each application by its own unique port number. A transport layer header contains the port addresses of both the source as well as destination applications. The port numbers are logical and not physical. The total number of unique ports possible in a single device are 65,536.



Source: http://www.informit.com

6. **Basic Software Building Blocks**: *Smartness* or *intelligence* of the cyber domain is primarily due to the various software applications which perform a variety of tasks ranging from analysis, interpretation, diagnostics, congestion control and routing. The software sub domain can be divided into four major components i.e. *protocols*, *operating systems*, *servers* and *application* software, as per details given below:

(a) **Protocols:**[6] These are a set of standard procedures which define the way communication and transactions take place within the network. Details of some important protocols are as under:

(i) **Internet Protocol (IP)**: The IP is the most important protocol which controls the movement of data packets along the network.

IP is an unreliable, connectionless service. By unreliable it implies that delivery of packets is not guaranteed and by connectionless it is implied that each packet is treated separately and is sent independently to its destination. The delivery of a packet to its destination can be either a *direct* delivery or an *indirect* delivery. In *direct* delivery, the source and destination belong to the same LAN while in *indirect* delivery, the source and destination are part of different LANs. In an *indirect* delivery, the packet goes from router to router till it reaches the router where the destination LAN is physically connected to it. At the final stage, the delivery happens as a *direct* delivery. The IP consists of four supporting protocols namely *Address Resolution Protocol* (ARP), *Reverse Address Resolution Protocol* (RARP), *Internet Control Message Protocol* (ICMP) and *Internet Group Management Protocol* (IGMP).

(ii) **Transmission Control Protocol (TCP):** The TCP provides a connection oriented service (a path between the source and destination is established before the flow of packets takes place). The packets in a TCP protocol are delivered in order without error from the source to the destination.

(iii) **User Datagram Protocol (UDP):** It is a connectionless protocol which is widely used for broadcast of audio and video content as the protocol uses less bandwidth and is quicker in comparison to IP or TCP.

(iv) **Hypertext Transfer Protocol (HTTP):** The protocol used to transfer a web page from a browser to a web server and vice versa. The secure version of HTTP is called HTPPS. The World Wide Web (WWW) is a repository of web pages spread all over the web and accessible over the internet.

(v) **File Transfer Protocol (FTP):** The FTP is a standard protocol provided by the TCP/IP suite for transferring a file from one host to another.

(vi) **Simple Mail Transfer Protocol (SMTP):** It provides simple email transfer facility from one mail server to another. The SMTP is used with Post Office Protocol Version 3 (POP3) protocol for transferring the mail from an Email server to a host machine.

(vii) **Simple Network Management Protocol (SNMP):** It is part of the TCP/IP suite and is an application layer protocol that is used to exchange management information between network devices.

(viii) **Domain Name Service (DNS):** It is a protocol that maintains a list of domain names with their corresponding IP addresses, allowing computers to query remote computers by their domain names rather than by their IP addresses.

(b) **Operating Systems:**[7] An Operating System (OS) is an interface between the user and the computer hardware. It performs a host of tasks to include file management, memory management, process management, security, handling input and output functions and controlling peripheral devices like device drivers and printers, etc. Some popular Operating Systems are: Linux Operating System; Windows Operating System; and VMS, OS/400, AIX, z/OS, etc. Android and IOS are two popular OS for mobile devices (smart phones and tablets).

A typical sequence of action of an operating system is:

(i) The OS executes an application

(ii) The Central Processing Unit (CPU) executes the instructions of that application. The OS is dormant.

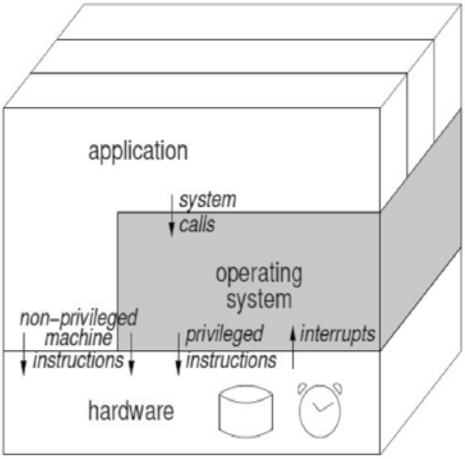
(iii) The system clock interrupts the CPU by clock interrupt handler (part of OS functionality).

(iv) The clock interrupt handler asks OS scheduler (part of OS functionality) to decide what to do next.

(v) The OS Scheduler decides for a context switch (another application to run in place of the first application).

(vi) Second application starts running. The OS is dormant.

(vii) The second application performs a system call (OS functionality) to read from a file.



Source: Notes on Operating System by Dr G Fetelson.

(viii) The system call activates a *trap* in the OS. The OS sets up for an Input/Output (I/O) function for the second application.

(ix) The OS then puts the second application to sleep till the time its I/O operation is completed and chooses another application to run.

(x) The third application starts running.

The above example highlights certain properties of the OS, which are:

(i) The OS are highly complex software that are structured around a particular system of hardware components.

(ii) OS are reactive. They keep on waiting for an event to occur. On occurrence, the OS react to that event in a pre-decided manner. Thus, unlike most of the software applications who receive an input, perform some function/s on that input thereafter produce an output and then shut down, the OS never terminate. They simply keep on waiting for the next event to occur. The OS events are of two types, *interrupts* and *system calls*.

(iii) Though it might seem that the OS are multi-tasking, in reality only one task at a time is being performed by the machine.

(iv) The OS present themselves to a software application as *abstract* machines that perform all the interface tasks and provide a simple standardised environment to all applications to perform their jobs. The OS also perform some level of abstraction, namely storage and retrieval of files, which are just stacks of memory in the computer.

(v) The OS perform *virtualisation*. The application does not access the system hardware directly but only through the OS. The OS gives each application the feel that the entire hardware of the computer (or machine) is available to that application while in reality it shares the same resource amongst different applications and optimizes resource sharing and availability. *Virtualisation* can also be implemented at Application layer level. *VMware* software application is an ideal example of this. It is a user level application that gets loaded on top of any conventional OS like Linux or Windows. Thereafter it creates a set of virtual machines which mimic the underlying hardware in entirety. Each of these virtual machines can boot a separate OS and run different applications.

(c) **Server:**[8] A *server* is a computer programme or a device that provides specific functionalities (services) to other programs or devices called '*clients*'. This model is called a *client-server* architecture and a *server* usually services a large number of *clients* while a *client* can also be connected to multiple *servers*. A *client* process may run on the same device or may connect over a network to a *server* on a different device. Typical *servers* include database servers, file servers, mail servers, print servers, web servers, game servers and application servers.

The *client* machine communicates with the *server* using simple lines of code known as *sockets*. In a *client-server* system, while the *client* keeps on entering and exiting the system, the *server* is always up and monitoring pre-designated ports for establishing communication with *client* machines. The *server* cannot anticipate which *client* will establish contact with it and when, so the onus of establishing contact always rests with the *client* machine.

In a *server-client* model, the following activities are performed by the *server*:

(i) **Step 1:** The *server* creates a *socket*. The OS creates a data location (file structure) to store all information about this specific communication channel between the *server* and *client/s* and allocates a file descriptor (file name) to serve as a handle to it.

(ii) **Step 2:** The *server* then binds this *socket* to a port number. The *server's* IP address along with the port number are used to identify this *socket*. The common services in a *server-client* model have got pre-defined port numbers which are known to all. For other services, the programmer has to specify the port numbers.

(iii) **Step 3:** The *server* then keeps on listening to this *socket* to monitor in case any service request is generated by the *client/s*.

In Unix OS, some of the port numbers for common services are as under:

Port Number	Service
21	ftp
23	telnet
25	Smtp(email)
42	Name server
70	Gopher
79	Finger
80	http(web)

The following steps are taken by the *client*:

(i) **Step 1:** The *client* also creates a *socket*.

(ii) **Step 2:** It then connects this *socket* to the *server socket* by giving the *server's* IP address and port number.

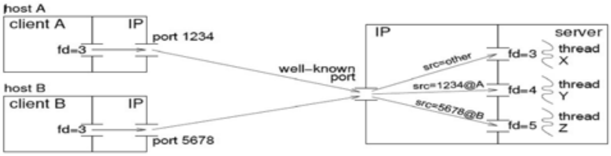
(iii) **Step 3:** A communication request is then sent to the *server*.

The *server* then takes the following additional steps:

(i) **Step1**: When it receives a request from a *client*, it creates a new *socket* and then accepts the request from the *client*.

(ii) **Step 2**: Connection is now established between the new *socket* (*Server* end) and the *client socket*. Data is then exchanged between both the machines.

The *server* creates a new *socket* to ensure that the pre-designated port number bound to a particular service is kept free to cater to requests originating from other *clients*.



A typical server-client connection set up mechanism

Source: 'Notes on Operating System' by Dr G Fetelson

(d) **Application Software:** This is the software that is used by the end user. It can be classified as *system* software (used for interaction with the computer) and *application* software (used for interaction with the end user). There are a wide variety of *application* software like word processors, spread sheets, data base, content & media editing and sharing platforms, etc. The *application* software can be written in high level language (written in a form which is closer to human language like English so that it eases writing of code by the programmer, is easy to port from one computer to another and easy to edit and debug) like *C, C++, Python, Jawa,* etc., or low level languages (*Assembly* language or machine code) which are set of instructions written for a specific architecture and hardware configuration of computer. The low level languages interact directly with the processors/microprocessors and are usually cumbersome to write, edit and debug.

7. **Security and Cryptography:**[9] As stated earlier, the internet was created without any underlying security considerations. At that point of time, nobody could imagine the sheer size, utility and impact that cyberspace would have on mankind. Over a period of time, developments in hardware and software coupled with rapid proliferation of cyberspace across the globe made users and developers sit back and realise the importance of protecting certain key aspects of their cyber domain. A rapid rise in spread of computer viruses and malware along with serious

cyber-crimes like financial scams and frauds speeded up the process of securing the cyberspace. But since, initially the cyber architecture, did not have any separate in built security layer(s), multiple ways of securing the cyber domain over each of the OSI or TCP/IP, layers were developed which were implemented on the basis of developer/user preferences. Some of the major cryptographic and security solutions being used in cyberspace are given in the succeeding paragraphs.

(a) **Application layer Security Standards/Protocols_**

(i) **Data Encryption Standard (DES)/Triple DES**: The DES was developed by IBM and was adopted as a US federal standard in November 1976. It is a symmetric block cipher which encrypts data in blocks of 64 bits using a key length of 56 bits. A total of 2^{56} key combinations are possible. Assuming that a single machine performs one DES encryption per μsec (10^{-6}sec), it would take more than 1000 years to break the combination. The triple DES uses three keys to perform three separate DES stages (encrypts with first key K1, then decrypts with second key K2 and finally encrypts with third key K3) to produce a staggering 2^{168} combinations which becomes immune to a brute force attack.

(ii) **Advanced Encryption Standard (AES): Rijndael Algorithm**: In October 2000, the US NIST adopted the Rijndael algorithm (Belgium origin) to replace the DES after a global search of over three years. The Rijndael is a block cipher created by Joan Daemen and Vincent Rijmen. The algorithm can work over data blocks of variable bit lengths (128, 192, 256, ...) using keys of variable length (128, 192, 256, ...). The only requirement is that the data and key length should be multiples of 32. This affords extreme flexibility to the algorithm and can be exploited over different hardware and software combinations.

(iii) **Rivest, Shamir and Adleman (RSA) Algorithm**: The RSA algorithm was invented in 1977 for encryption and digital signatures and is the world's first public key cryptosystem. The algorithm uses a set of two keys (public and private keys). Messages are encrypted using the public key and decrypted by using the private key (known only to the concerned party). Generation of public – private key pairs is relatively simple and the strength of the algorithm is derived by using keys of large length i.e. 1024, 2048, 3072 bits. The RSA cryptosystem is about 100 times slower than the DES algorithm.

(iv) **Pretty Good Privacy (PGP)**: The PGP was invented by Philip Zimmermann in 1991. It uses a combination of symmetric and asymmetric (public key) algorithms to provided security to e-mail services. At the sender end the following actions take place: firstly, a random 128 bit symmetric *session key* is generated for each individual message. Secondly, this *session key* is encrypted using the public key of the receiver (using RSA algorithm). Thirdly, the message is encrypted with the *session key* using Triple DES (or any other symmetric key cipher like IDEA or CAST 128). Fourthly, the sender then transmits the encrypted *session key* and message to the recipient. The receiver first decrypts the *session key* using his private key (RSA) and thereafter decrypts the message with the *session key* (Triple DES).

(v) **Hash Function:** One of the major concerns in cyberspace is ensuring data integrity i.e. to say that the message once sent by the sender is not manipulated, errors introduced or altered in any way during the entire chain of transmission and retransmissions till it finally reaches the recipient. Hash functions also called *message digest* or *one way encryption* are cryptographic algorithms that provide a digital fingerprint of the contents of a file to ensure its integrity to the recipient. Hash functions work by inputting the entire contents of a file to the algorithm, which in turn creates the fixed length hash value. This implies that even a single error in the file contents will alter the hash value. The receiver has to just recalculate the hash value of the received file and compare it with the hash value sent by the originator of file to confirm whether the contents of the file are original or otherwise. Hash functions are also used for encrypting passwords. Commonly used hash functions are *Message Digest (MD)* series and *Secure Hash Algorithm (SHA)* series.

(vi) **Secure Electronic Transaction (SET):** These are a set of protocols developed by Visa and MasterCard in 1996 for protecting credit card transactions. SET uses two pairs of asymmetric keys for encryption/decryption as well as for verification of digital signatures. SET establishes a complete ecosystem with major participants being the card holder, issuer, merchant, payment gateway and certification authority to provide seamless end to end confidentiality (ensured through encryption by DES), integrity (Using RSA Digital signatures with SHA-1 hash codes), card holder authentication (through Digital signatures) and merchant authentication (through Digital certificates and digital signatures) of financial data.

(b) **Network Layer Security Standards/Protocols:** *IPsec* is a set of protocols developed by the IETF to provide security services at the IP layer of TCP/IP architecture. The major services provided by IPsec are encryption of user data, message integrity checks, protection against replay cyber-attack and negotiation of security algorithm and keys among various nodes. The two primary protocols being used are the Authentication Header (AH) and Encapsulation Security Payload (ESP) while the Security Association (SA) provides the security frameworks for negotiating security algorithms and keys between different communication nodes.

(c) **Transport Layer Security Standards/Protocols**: *Secure Socket Layer* (SSL) is a transport layer set of two protocols (SSL Record protocol and SSL Handshake protocol) which were created by Netscape Communications in 1995. The protocol provides client/server systems to communicate securely and prevents eavesdropping, tampering and forgery of messages. The SSL Record protocol is implemented on top of the TCP block. The SSL Record protocol collects the upper layer messages and then fragments them into manageable blocks of fixed data length, thereafter it compresses the data (optional), adds Message Authenticating Code (MAC), encrypts using symmetrical block cipher (DES, Triple DES, IDEA, etc.) adds a header and sends the resultant block to TCP for further processing and transmission. The SSL Handshake protocol lies above the SSL Record protocol and is responsible for initiating the communication between the client and the server by first sending the client *Hello* message followed by the server *Hello* message after which the server authentication (verification of server's digital certificates) and key exchange takes place and finally the client authentication and key exchange happens. The SSL handshake protocol ensures that a mutually acceptable protocol version, encryption algorithm and encryption keys are agreed upon before the first message is exchanged between the client and the server.

(e) **Physical layer Security**: *Firewall* is a group of application suites that are implemented on a device or a group of devices with the aim of providing security services between different networks. It primarily consists of filters and gateways and screens the incoming and outgoing traffic for dangerous and inappropriate content which it disposes off as per laid down policies. Firewalls provide a host of services including access management, event logging, network protection and implementing Virtual Private Networks (VPN). They can be classified into three main categories, packet filters, circuit level gateways and application level gateways. Some of the important firewall terminologies are:

(i) **Bastian Host**: This is the device which is directly connected to the un-trusted network (internet). The Bastian host is configured to withstand cyber-attacks from both incoming as well as outgoing traffic and checks the traffic as per the laid down firewall policies

(ii) **Proxy Server**: A proxy server is used to communicate with servers of untrusted network on behalf of trusted network clients. Proxy servers are established and closed based on client request and are not permanent in nature. Internet traffic between the proxy server and servers of untrusted networks takes place using the *SOCKS* protocol.

(iii) **Choke Point**: These are the pre designated points where the traffic of un trusted network and trusted network meet/get exchanged. The choke points are extensively monitored to ensure that all inbound/outbound traffic is carefully screened, logged, filtered and discarded.

(iv) **De-Militarised Zone (DMZ)**: A DMZ is a buffer network placed between the trusted and the untrusted networks. The DMZ network is also referred to as the perimeter network and provides an additional layer of security to the trusted network.

Notes

1. https://en.wikipedia.org/wiki/OSI_model, accessed on September 19, 2018.
2. https://en.wikipedia.org/wiki/Internet_protocol_suite, accessed on October 1, 2018.
3. https://en.wikipedia.org/wiki/Satellite_Internet_access, accessed on October 4, 2018.
4. https://www.fiberoptics4sale.com/blogs/archive-posts/95146054-optical-fiber-tutorial-optic-fiber-communication-fiber and https://www.tutorialspoint.com/principles_of_communication/principles_of_optical_fiber_communications.htm, accessed on October 9, 2018.
5. http://www.informit.com/articles/article.aspx?p=2272153&seqNum=5, accessed on October 10, 2018.
6. Man Young Rhee, *Ínternet Security Cryptographic Principles, Algorithms and Protocols,*John Wiley and Sons, 2003 edition, Chapter 2.
7. Dr G Fetelson, *Notes on Operating System*, Jerusalem, School of Computer Science & Engineering, the Hebrew University, 2011.
8. Ibid.
9. Note 2.

Appendix B

ESSENTIALS OF AI

1. **Introduction to AI:** The study of AI is derived from three fundamental streams of mathematics namely logic, computation and probability[1]. Though the concept of logic can be said to have been originated during the time of Socrates, but George Boole (1815-1864), the inventor of Boolean logic and algebra, can be said to be the pioneer of mathematical logic which is being used till date. In 1931, Gödel in his "incompleteness theorem" proved that there are some functions on integers which cannot be represented by an algorithm or in other words cannot be computed. Alan Turing (1912-1954) thereafter tried to classify the functions which could be computed and this led to the Church-Turing thesis, which stated that all computable functions can be computed by the Turing machine (a mathematical model of computation which manipulated symbols on a strip of infinite length tape as per a set of rules); and also there were some functions (like no machine can tell in general whether a programme will return an output or run forever given a particular input) which cannot be computed by the Turing machine. Another aspect of the notion of computability was "tractability" i.e. a problem was said to be intractable, if the time required to solve instances of a problem grew exponentially, with the size of instances. This led to the discovery that there were certain class of polynomials whose solving complexity grew exponentially even with a small increment to their order and it was better to solve a set of tractable sub problems rather than solve a single intractable one. The Steven Cook and Richard Karp theory of NP-Completeness provided a method to classify problems, that were intractable. Finally, the theory of probability provided the means to reduce complexity of tractable problems by giving a reasonably correct response to a computationally complex problem, in an acceptable time frame.

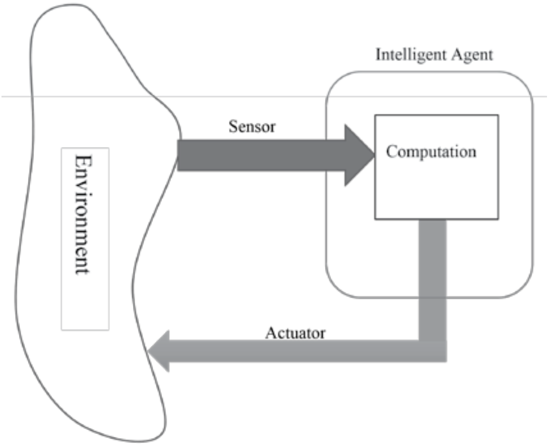
A key contributor towards the development of AI was Herbert Simon (1916-2001) who won the Nobel prize for economics in 1978, for his work in the field of "Satisficing" which propounded that human behaviour in the real world was for the achievement of models which make "good enough" decisions and not exact decisions. Other areas of study from which AI draws a lot of inspiration are the fields of "Preferred outcomes" or "Utility theory" from economics, decision theory, game theory, operational research and neuroscience.

Summit or OCLF-4 is a supercomputer developed by IBM for the Oak Ridge National laboratory and acknowledged to be the fastest supercomputer in the world in November 2018.[2] A comparison between Summit and the human brain is given below:

Attribute	**Supercomputer Summit**	**Human Brain**
Computational Unit	10^{14} transistors	10^{11} Neurons
Storage Unit	2 X 10^{17} bit Random Access Memory (RAM)	10^{11}Neurons
Operations per second	2 X 10^{18}	10^{17}

It is evident that the supercomputers have reached or exceeded the human brain's capacity. However, whether they have achieved the brain's intelligence or creativity, is an open question. Some in the AI field, like Ray Kurzweil[3] (author of *The Singularity is Near* and *How to create a Mind*), term the phenomenon when super-intelligent machines overtake the human potential of intelligence and creativity *"Singularity"* and argue that the super intelligence created by these machines will grow exponentially, with far reaching consequences for the human race.

2. **The AI Model:** The AI machine can be considered as being an intelligent agent, which perceives a given environment through its sensors and after carrying out computational work on its sensory inputs, gives directions to its actuators who further carry out the specified work on the environment.



An agent's Percept refers to the input received by it, at any given instant of time. A Percept Sequence refers to the complete history of the inputs received by the agent till now. The agent's choice of action at a particular instant will depend on the Percept Sequence, till that instant only. By mapping the agent's actions for every possible Percept Sequence we would be able to define the actions, which the actuator is allowed to do to the environment.

AI can therefore be defined as "The design of intelligent agents which based on the sensory inputs given to the agent provide non trivial actuator outputs to the environment".

A rational agent is one that does the right things. In simple terms, if the action performed by an intelligent agent on the environment based on the percept sequence it has received, results in the environment changing into desirable state(s) which can be performance evaluated, then that agent can said to be a rational agent.

Another important feature associated with a rational agent is autonomy. This implies that the rational agent must have the ability to learn from the percept sequence in order to enhance its performance evaluation without any other stimulus. Initially, the intelligent agent can be fed with certain information, a-priori, but as it continuously performs its tasks on the environment it self-learns and thus self-improves, in performing its task.

The first step in designing an intelligent agent is to fully specify the task environment, which is the description of Performance, Environment, Actuators and Sensors (or PEAS for short). The PEAS of an autonomous car could be as under:

Performance	**Environment**	**Actuators**	**Sensors**
Speed, comfort, time, collision free, safety, overall wear and tear	Road, streets, highways, garage, basement	Steering, brake, acceleration, gear, lights, lamps	Radars, navigation, camera, microphone, inputs from engine, machinery, etc.

3. **Type of Environments:** A fully observable environment is one in which the sensors are able to accurately provide all relevant inputs (percept sequence) to the agent in order to perform their tasks. On the other hand, an environment can be said to be partially observable, in case of inaccurate sensors or when some environmental states have still not been reflected in the percept sequence to the agent. An unobservable environment is, when there are no inputs from the sensors to the agent. Let us take the example

of an agent tasked to identify items from the conveyor belt and then to pick up and place them in a particular box. In case all the sensors are accurate and functional, then the working environment can be said to be a fully observable environment. On the other hand, the environment presented to an autonomous car can be said to be partially observable as all the states of the environment might not have been presented to the agent.

Environment can also be classified as a single agent or a multi agent environment. A single robot picking up items from a conveyor belt, is an example of a single agent environment, while multiple autonomous vehicles plying on a highway are an example of a multi-agent environment. Environment can also be deterministic or stochastic. In case the environmental state can be fully arrived at, from its previous state and actions of the rational agent, then it is a deterministic environment else, it's a stochastic one. It is quite evident that an intelligent agent in a fully observable and deterministic environment will make no assumptions while producing an actuator output, in other words it will give a non-probabilistic output.

Environment can also be episodic (when action of agent is only dictated by the present percept) or sequential (action of agent is determined by the percept sequence). It could also be static/dynamic or discrete/continuous. Thus, different working environments will dictate the degree of relative hardness and complexity relating to the intelligent agent's ability to provide rational actuator outputs to the environment, resulting in enhanced performance results.

4. **Types of Agents:** The aim of AI is to write agent programmes that act rationally and produce the desired output of actuator, after receiving percept sequence inputs from the sensors. The major challenge in designing AI systems, is that if we start tabulating all the sensor inputs over a period of time and thereafter carry out analyses of those inputs to produce output of the actuators, then we firstly run out of memory space. We also find it computationally increasingly difficult to calculate desired outputs for the actuators and performing the steps within realistic time frames, becomes almost impossible.

Therefore, the key to a successful AI programme is that it produces the desired actuator output by using the barest minimum memory, computational power and time. There are four types of AI programmes that are used to fulfil the above criteria. Details of the same are given in the following paragraphs.

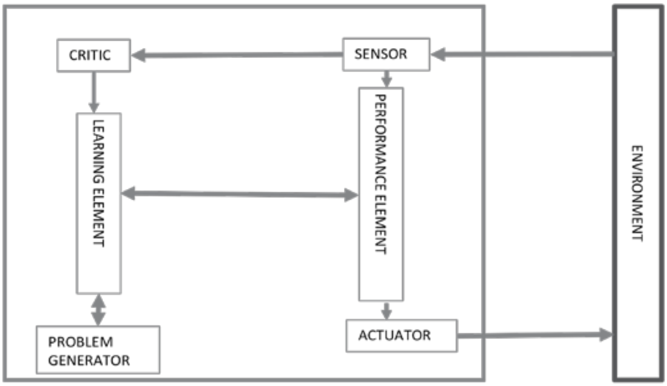
(a) **Simple Reflex Agents:** These agents provide actuator output based on the current percept only. The programme creates a set of "condition-action rules" wherein the sensor defines the condition and the corresponding action results in the desired operation by the actuator. The task of identifying a faulty part on the conveyor belt by an assembly line robot and discarding it, would fall into this category of agents. As can be seen, a simple reflex agent can only work in a fully observable environment.

(b) **Model based Reflex Agents:** These agents are used in a partially observable environment. Apart from the current percept, the agent gathers certain key indicators/features from the percept history to formulate a model of the environment. Thereafter, based on this model of the environment, it issues a set of instructions to the actuator, based on formulated "condition-action rules". For example an autonomous car may reduce speed when it observes that the car ahead of it has reduced its separation distance.

(c) **Goal Based Agents:** In a goal based agent model, the agent is provided with a goal which needs to be achieved. Therefore, apart from the current state of environment (as obtained from Model Based reflex agent), it would also need goal based information, which would allow it to compute and choose the desired action (from condition-action rule set), that would facilitate it in achieving its goal.

(d) **Utility Based Agent:** A utility based agent can be deemed to be an improved version of a goal based agent. While a goal based agent may be primarily interested in achieving its goal in minimum steps, a utility based agent would try to optimise multiple performance parameters in order to achieve its goal. For example, a goal based autonomous car may be able to reach its destination by taking the shortest route, a utility based autonomous car might optimise the distance, time taken, quality of road, density of traffic and weather condition, to arrive at an optimum solution for reaching the destination.

(e) **Learning Agents:** A learning agent is one wherein at first the agent performs sub optimally in the initial unknown environment and thereafter improves its performance (measured against pre-set performance parameters) after each subsequent interaction with the environment. The learning agent can be divided into two interacting modules i.e. the learning element and the performance element modules. The learning element module consists of the critic, feedback agent and problem generator while the performance element consists of the feedback agent and actuator. Both the learning element and the performance element are connected to each other and the environment. Input received from the environment is compared with the performance parameters by the critic and a feedback is given to the feedback agent as well as the problem generator of learning element. The problem generator suggests certain actions which can be taken by the performance element to optimise its performance. These suggestions are passed on by the learning element to the performance element, which then carries out suggested actions through the actuator and the new percept from the environment is generated which is again fed to the learning and performance elements and the cycle continues.



Deep Learning is based on neural networks where millions of software based calculators called "neurons" form multiple layers, with each layer performing complex tasks like pattern recognition. These layers are able to exchange information amongst themselves leading to the parallel processing of large quantity of data and more accurate results. The neural network first makes inferences out of the data fed to it, compares it with pre-processed learning data set and after multiple learning cycles trains itself to make better predictions to ensure more accurate outcomes. Deep learning based networks also require less pre – processing of data sets, in terms of annotation by humans. In order to minimise the error of prediction, the gradient descent or back propagation algorithm is resorted to.

(f) **Knowledge Based Agents:** The central component in a Knowledge Based Agent is the "Knowledge Base (KB)". A KB is a set of "Sentences (Sentence is a technical term and not to be confused with Sentence of any language)". Each sentence is represented in a language known as the "Knowledge represented language". Important characteristics of a KB are that you can add a new sentence (TELL) and query the KB (ASK).

Three major steps are executed whenever the KB agent is invoked. In Step 1, the current percept of the environment is informed to the KB

(TELL). In Step 2, the agent ASKs the KB which action is required to be executed. The KB is then subjected to extensive reasoning to find out the optimum action required to be executed and would invariably refer to the updated KB as well as previous outcomes of similar problems...In the final step, once the action for execution is intimated, it is not only executed but the KB is also updated by adding a new sentence (TELL).

The sentences in KB are written as per "syntax" of the represented language. Syntax is the correct way of writing sentences. "Logic" is the underlying true meaning behind the sentences. For example if a sentence is represented in correct syntax as "X + Y = 5", then if the value of X is 2 and Y is 3, then the logic is correct but for a value of X = 2 and Y = 1, the logic is incorrect. "Entailment" means the logical transition from one sentence to another. Entailment leads to "logical inference" and gives rise to the "inference algorithm". An inference algorithm is called "sound" if it produces only entailed sentences and called "complete" if it can derive any sentence that is entailed. Thus, if a KB is considered true in a real world then the sentences that are derived from this KB through sound inference algorithms are also true in the real world.

Another important facet of a KB is the Truth Maintenance System (TMS). Based on fresh inputs fed to the KB, it is quite possible that certain earlier inferences made by the inference algorithm become wrong and need to be changed. This is known as Belief revision. The task of the TMS is to retract the statement containing the wrong inference and also subsequent statements, which were made based on the earlier wrong inference. One way to do this is by numbering each sentence, as it is fed into the KB and after detecting a wrong inferred sentence removing all sentences, which came after that sentence. Thereafter, all sentences other than the ones which contain inferences drawn from the wrong inference sentence, are added back into the KB. This method is quite cumbersome and difficult to implement in large KBs which are being constantly updated. The Justification-based Truth Maintenance System (JTMS) is a simpler and elegant method to carry out belief revision. In this, each sentence is annotated with the set of sentences denoting the justification from which it was inferred. In case of a wrongly inferred sentence, only those sentences which were inferred on the basis of that sentence will be removed from the KB.

5. **Planning System:** A planning system essentially consists of actions required to be done from the initial state till the goal state in order to meet the intelligent agent's objective. Thus, any problem will consist of the initial state, actions possible from the initial state to intermediate state along with their outcomes and the goal test to determine whether a given state is the goal state or otherwise.

The Planning Domain Definition language (PDDL) is a tool used for implementing the planning system. In the PDDL all states and actions are represented as a set of variables. An action "schema" would completely define a particular action and consist of the action name, list of all the variables, the precondition rules and effect caused by that action.

There are three main approaches to automated planning. First, translating to a Boolean Satisfiability (SAT) problem. Second, forward state-space search with heuristics and lastly, search using a planning graph.

6. **Search Problems:** One of the most common problem which uses AI to arrive at solution are the various Search problems. Such problems range from finding a route for travelling from the start point to the destination, looking for keywords on the web or text, web crawling for hashtags and websites, etc. All the search problems have a definite goal to be achieved and start from an initial state. The search algorithm then works out a sequence of actions which need to be executed to move from the initial state to the goal defined state.

A search problem can therefore be sub divided into five components. First, the initial state (the state from which the agent is trying to solve a search problem). Second, the various action options available for execution from the initial state. Third, the outcomes which are available after executing each action option (This is also called the transition model). Fourth, the *S*tate Space which is arrived at from the initial state after executing a particular action option using the transition model and lastly, the Goal Test to verify whether a particular state space is the final goal state or not. Thus, a number of paths can be arrived at from the initial state to the goal state depending on the number of action options available at the initial state and all subsequent states till the final goal state. Therefore, the initial state, goal state and all the intermediate states form a directed network or graph, where all the states are the nodes and the link between the nodes are the actions.

A typical search problem has an initial state and associated path cost along each intermediate state. By adding various path costs as one moves along multiple states one after another to reach the final goal state gives rise to step cost and an optimum solution can be considered in which the step cost is the least amongst all the options considered for reaching the goal state from the initial state.

Some of the real world problems which utilise AI to solve search problems are optimising flight travel schedules especially involving multiple hops and airlines, touring problems (going from one place to another), the Travelling Sales Person (TSP) problem (it is a NP hard problem and the solution involves the sales person visiting each city only once), Very

Large Scale Integrated (VLSI) circuit board solutions for packing multiple miniature devices and circuits including movement of circuit board drills, robot navigation and movement along an assembly line, etc.

The search problems fall under the tree search category in which although the end goal is the same (to optimise the path from initial state to goal state) but different search strategies (in terms of algorithms) are employed to optimise memory, computational complexity and time requirements.

A Breadth-First search algorithm is a simple search algorithm wherein all successors of the root node (initial node) are expanded first, followed by their successors and so on … Though breadth search algorithm is capable of arriving at an optimum solution however, it fails to deliver on the memory, complexity and time fronts and is nearly impossible to implement in real world problems.

The Uniform Cost search algorithm first expands the node with the lowest path cost and adds an additional check by verifying in case a shortest path is discovered to the forward state from an earlier state, which might not have the shortest path cost to the initial state. The algorithm thus continues as a comparison between two paths, till the final goal state is achieved. Other search algorithms are the Depth-First, Depth-Limited, Iterative Deepening and Bidirectional.

A heuristic function is a real number which is an estimate of the least path cost to reach the goal state from the initial state. A heuristic function can be arrived at by solving a simpler problem in comparison to the actual problem, storing a pre calculated figure or using experience (path costs arrived after running the problem set through multiple iterations). The heuristic function helps in arriving at best case solutions with minimum utilisation of memory, computational power and time. Some of the algorithms using heuristic functions to arrive at a goal state are greedy best-first search, A* search, iterative-deepening A* and recursive best-first search algorithms.

7. **Adversarial Problems:** These types of problems are also known as "games" and are played in a multi-agent based competitive environment. The impact of the agent's action on one another can be significant and their goals are generally in conflict with each other. Also, some agents could be collaborating with each other, while others may be in conflict.

Most of the AI based games like Chess or Go are zero sum games where the net result is always one i.e. one agent wins and the other loses, or they draw. These games are also fully observable, turn taking, two player and deterministic. Playing games has fascinated AI researchers because first, games are difficult to solve and secondly, penalty for making sub optimum decisions is very high. However, solving complex games involving multiple players which are partially observable and not fully deterministic is an altogether different ball game.

A game can be considered as a special case of a search problem having an initial state, players, action set (possible allowed moves from a given state), result (transition model of a particular move), terminal test (to see whether a game has finished or not) and a utility function (the numerical value assigned to a player after the game ends). The game tree is defined by the initial state, action set and result function, wherein the nodes are the various states which the player takes from the initial state till the end state and the edges or branches are the various moves, which are possible between different states.

Stochastic games are those where an element of uncertainty (like a throw of dice) is introduced in the game. Thus additional chance nodes apart from max and min nodes are introduced in the game tree thereby increasing its complexity in comparison to fully deterministic game trees of chess or tic-tac-toe.

A large number of algorithms exist for playing different games along with strategies to optimise memory, computational complexity and decision time. One such algorithm is the *minmax* algorithm to denote two players; *min* and *max* who are in competition with each other. The states taken by *max* and *min* would depend on the previous states taken by the competing player and the subsequent move options available in order to either maximise or minimise the utility function which will ultimately result in a win, loss or draw.

Needless to state that the complexity, spread and depth of the game tree increases exponentially when we play multi-player games with players continuously competing and collaborating with each other.

Generative Adversarial Networks (GAN) are a set of opposing neural networks. One network is the Generator while the other is Discriminator. The Discriminator is fed with the annotated learning data set as well as the output of the Generator. The aim of Discriminator is to assign a probability to the Generator output whether it mimics the output of the annotated learning set or not while the task of the Generator is to fool the Discriminator into believing that its output is same as that of the learning data set. This translates into a cop and thief game with the Generator as the thief and the Discriminator as the cop. Both Generator and Discriminator continuously learn from each other and thus are able to improve the predictive outcome manifolds.

As stated earlier Alfa Go, Google's AI based learning system was able to defeat Lee Seedol, the reigning Go professional champion in March 2016. What is more surprising is that AlfaGo's successor AlfaGo zero with no human training and access to data sets was able to defeat AlfaGo, 100 games to zero, learning from scratch. AlfaGo zero used GAN based algorithm that used "reinforcement learning" to play against itself and thereby continuously self-improved and was able to defeat all other versions of AlfaGo programmes in a matter of just 40 days of self-learning. It proved that the most important component of an AI system is the algorithm and not the data or computational power.

Contract bridge is a partially observable environment competitive game of cards played by four players, consisting of two teams of two players each. Bridge is a more difficult game than chess or Go to play as it combines skills of logic, reasoning, maths and inter personal communications to collaborate and win the game by deception and surprise. World's fourth richest man and Billionaire investor Warren Buffet is a diehard competitive Bridge player who plays up to 12 hours per week. He has said that:

Bridge has got to be the best intellectual exercise out there. You're seeing through new situations every ten minutes.... In the stock market you don't base your decisions on what the market is doing, but on what you think is rational.... Bridge is about weighing gain/loss ratios. You're doing calculations all the time[4].

For the last 22 years since 1997, the American Contract Bridge League has been organising the World Computer Bridge Championship amongst competing computers. The 22nd World Computer Bridge Championship was held from September 29, 2018 to October 4,2018. A total of nine teams competed in the championship including TCS Bridgebot from India. A central server or Table Manager (TM) was connected to four computer terminals representing the players and cards were distributed by the TM to the players. Initially the key features of opponent players are fed to the computers manually and thereafter the play proceeds automatically, between the TM and four computers till the match is decided. The championship was won by *Wbridge5* of France who has won the championship third time in a row. **An AI based robot bridge playing team is yet to win a competitive game of bridge against a team of humans.**

8. **Knowledge Representation:** Ontology Engineering can be considered as the study of representing various objects, their attributes and relationships in order to categorise them for use in a Knowledge Base. Objects are grouped under categories. Each category has typical characteristics and are hierarchical in nature which gives rise to taxonomical hierarchies. There are relationships within categories as well as between different categories. For example, man is a sub category of homo sapiens which is a sub category of mammals and which in turn is a sub category of living beings.

Categories can be of different kinds. Some have strict definitions like "straight line (shortest path between two points on a flat surface)".

However, most of the categories found in the natural world do not have clear cut definitions. To circumvent this problem and assist the logical agent, categories or sub categories are represented as *typical ( )*. This implies that most of the objects found in this category/sub category would fulfil the *typical ( )* attributes. Another concept about categories is pertaining to scales of measurement of a particular category. Some attribute of categories like length, weight, height etc. can be easily represented in numerical form. Certain attributes like deliciousness, degree of difficulty/beauty, etc. are difficult to represent numerically, but they can be compared with different members of the same category and this order of comparison (ascending/ descending), can then be used as an input for the logical agent. Categories can also be described in terms of event calculus (state of an event with respect to a particular instance of time).

In order to quantify the various shades of truth (possibility, necessity, obligatory, permissible, it is known, it is believed etc.) as well as make mathematical sense of statements used in real world to the logical agent, modal logic[5] in inference algorithms is used.

Categories are the basic building blocks of Knowledge Representation. There are two ways to construct categories and specify relationships between various categories. These are: The Semantic network, which gives a graphical representation; and the Description logic, which provides the formal language to construct and work with categories.

9. **Working Under Uncertainty:** As brought out earlier, the intelligent agent maintains a set of belief states and all possible actions arising out of these states, based on the percept sequence it receives from its sensors. In case of partially observable environments (environments with elements of uncertainty), the agent is required to maintain track of all possible belief states along with their corresponding actions. In real world systems, which are by and large partially observable, this creates enormous strain on memory and computation power and finding a solution in reasonable time frame becomes almost impossible. To achieve optimum and real world solutions, the inference algorithms make use of probability to remove uncertainty as well as manage the memory and computational requirements of the system.

In order to arrive at a best case solution in a partially observable environment, the intelligent agent must first be able to arrive at all possible solutions that satisfy the goal state and there after optimise the utility function of each solution to arrive at the optimum solution. However, in case the probability of success of each solution is different, then to arrive at the decision of optimum solution, the probability of each solution also needs to be factored in. Therefore, it can be stated mathematically that *Decision Theory = Probability theory + Utility theory*.

A Bayesian network (also called belief network or decision network) is a graphical model where each state is represented as a node and the actions represented as probabilistic functions, based on conditional dependencies which are used to connect different nodes. Bayesian learning is a method of learning from the probability distribution of data presented to the intelligent agent as percept sequence. The learning of such types of probability models from the data fed to the intelligent agent, is called density estimation. Initially, a prior probability distribution called hypothesis prior is fed to the intelligent agent. Subsequently, the probability distribution undergoes changes as data continues to be fed to the intelligent agent.

Bayesian networks are important in AI as effective inference algorithms make use of Bayesian networks to arrive at optimum decisions as well as further improve the algorithm through learning. A large number of methods like direct sampling and Markov Chain Monte Carlo algorithms are utilised to work out the probabilistic distribution over large Bayesian networks. Over a period of time, the probabilistic approximation keeps on improving as TMS carries out *B*elief revision based on feedback generated by learning systems.

Fuzzy logic is a method for arriving at numerical values of not well quantified descriptions. For example, Shiela is very beautiful. We make use of fuzzy logic to quantify beauty and fuzzy rules to assign a numerical value to Shiela's beauty.

Another real world challenge facing the inference algorithm is time. Till now, we have assumed that the nature (attributes) of state does not change with time. However, real world is filled with several instances where the nature of state is quite dynamic and time dependent. Let us consider the condition of a cardiac patient whose various parameters like blood pressure, pulse rate, blood sugar levels, etc. keep changing and have a significant correlation to the type and quantity of medication to be had. Thus, when working with time as a variable, we need to perform the following tasks. Firstly filtering, which is calculating the most probable present belief state. Secondly, prediction which involves calculating the probability distribution over all the possible future belief states. Thirdly, smoothing which calculates the probability distribution from the present state to the past states. And lastly, most likely explanation which predicts the most likely path taken from previous states to reach the current *state*. Hidden Markov Models and Kalman Filters are some of the techniques used by inference algorithms when working with time as a variable.

10. **Decision Making by Intelligent Agent:** As stated earlier, decision optimisation by the intelligent agent is carried out by optimising the

probability and utility function of a given path along the Bayesian network from the initial state till the goal state. Calculation of accurate utility functions and probability therefore assumes utmost importance in AI based decision systems. However, accurate calculations of both the above parameters over various action states for real world problems is very difficult.

Calculations of utility functions can suffer from over simplification of real world problem, computational complexity of the problem or inadequate sampling size of data available for a particular action state. To make matters more complicated, behaviour economists have proved beyond doubt that humans are "predictable irrational"[6].

One common currency in behaviour economics is "micro mort". One micro mort is the probability of one : one million of death. What is interesting is that for the same odds for two different situations people tend to quote different numbers while taking the risk. For example, persons when asked to participate in a new user drug trials, where the probability of death due to side effects is one in a million, will quote a very hefty sum sometimes running into thousands of dollars. On the other hand, there is well established empirical evidence that driving a car in USA for 250 km results in a risk of one micro mort. The total risk over the entire life cycle of a car (one lakh km) works out to 400 micro mort. A large number of surveys have shown that customers are ready to shell out $10,000 extra for a car's safety features, if it reduces the risk of death by half. In other words, cost of risk per micro mort while commuting by personal car works out to $50.

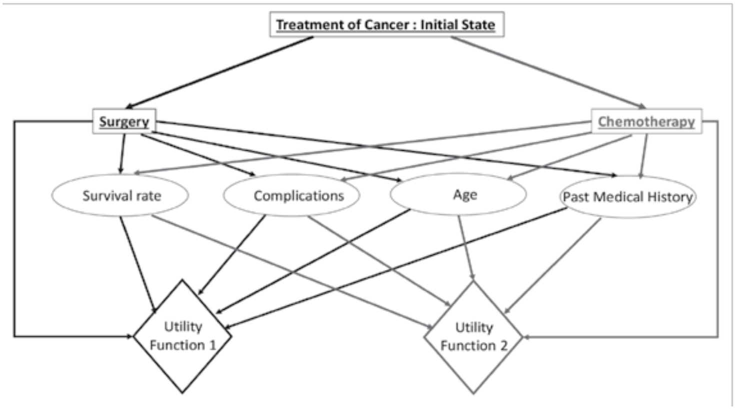
Another aspect of human behaviour is the certainty effect which gives rise to Allais paradox.[7] If a given sample size of persons are given two choices i.e. Choice 1: 80 per cent chance of earning Rs 4,000 and Choice 2: 100 per cent chance of earning Rs 3,000, then by and large the sample subjects make Choice 2, in spite of it being a less favourable option. Humans by nature are prone to a number of personality related biases which colour their decisions. Some of these biases are Ellesberg paradox, ambiguity aversion, framing effect and anchoring effect.

Multi attribute utility theory deals with decision making for complex and strategic problems where a large number of attributes need to be optimised to arrive at a rational decision. Selective narrowing down of competitive options is carried out by subjecting them to number of evaluation models like stochastic dominance and multiplicative utility functions.

11. **Representation of Decision Networks:** A decision network is a pictorial and essential representation of the current state, available actions from the current state, resultant states post action and their associated utility function values. It is represented by three types of nodes:

(a) **Chance Nodes (Oval)**: These are the various parameters or attributes which are being evaluated for decision making.
(b) **Decision Nodes (Rectangular):** These represent different options available for decision making**.**
(c) **Utility Nodes (Diamond)**: It gives the cumulative utility cost of a particular choice/option.

A Simplified Decision Network on Line of Cancer Treatment



12. **Learning Systems:** As stated above, an intelligent agent is said to be learning if after completing a task, it obtains feedback from the environment, makes relevant deductions from the feedback and subsequently improves upon its existing methodology, to provide better results and performance. Learning algorithms in AI are extremely useful and necessary for the following reasons. First, system designers and programmers are unaware of all the states which are possible in a given problem. For example, playing chess or Go to defeat world champions is not known beforehand by the AI programmer. Second, predicting future states which are time dependent is not possible. For example, the future fluctuations in stocks and their impact on market cannot be decided beforehand. Lastly, programmers are themselves clueless about the optimum method for solving a given problem. Example, facial recognition.

There are four important questions which need to be answered prior to designing an intelligent learning agent. First, which components of intelligent agent need to be improved? Second, what prior knowledge is already available with the agent? Third, what representation is to be used between the data and component? Lastly, the feedback to learn from?

The components that can be improved include: condition-action mapping of states; environmental view based on percept sequence;

information about evolution of environment over time; updated utility function of various states and information concerning various state/s which maximise overall utility function.

Feedbacks are of three types. In unsupervised learning, the agent tries to detect patterns in input without any direct feedback being provided to him. For example detecting common words being used by a particular author in his sentences. Reinforcement learning follows the carrot and stick method, wherein the agent is rewarded for a suitable action and punished for a wrong action. For example getting additional utility function points, in case a particular state results in a win in a game of chess. In supervised learning, the agent is shown a number of input-output examples and learns to construct a function which results in similar input-output pairs.

Computational learning theory is a fast emerging field which deals specifically with supervised learning algorithms. In this, the intelligent agent is given labelled input samples with specified attributes (say good or bad) during the learning phase and subsequently the agent is required to give a classifier as output which is nothing but labels the fresh samples being given to it as input. These samples would not only contain those which were introduced to the agent during the learning phase but also those samples, which are being introduced to the agent for the first time. The overall aim of the learning process is to ensure that the classifier produces least errors. Computational learning theory also predicts whether a given problem is solvable in polynomial time or not and whether it is feasible to design a learning algorithm, for a given problem.

Data sets and annotation of data are the key requirements of a learning based AI system. An AI system which has been subjected to learning from a vast data set with annotated data will perform more efficiently, as compared to a system which has been subjected to training from a lesser data set. Annotation or the process of labelling the data in the data set so that the AI system can learn and recognise a particular pattern to represent a specific characteristic/object is performed by humans and is a very time consuming process.

Explanation Based Learning (EBL), Relevance Based Learning (RBL) and Knowledge Based Inductive Learning (KBIL) are some of the methods used to implement learning algorithms where prior knowledge is available.

Notes

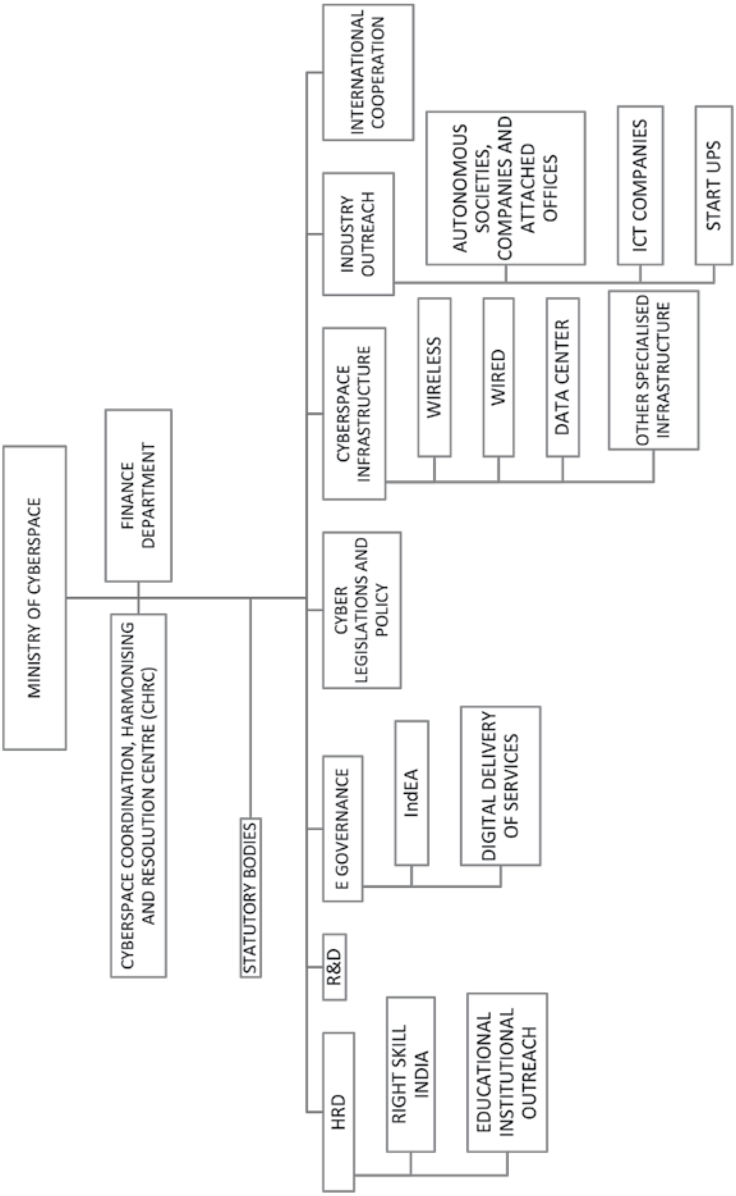
1 Stuart J. Russel and Peter Norvig, *Artificial Intelligence A Modern Approach*, Third edition, Prentice Hall, 2010. The book has been extensively referred for explaining the fundamentals of AI.

2. Details on *Summit* can be obtain*ed at* https://www.ibm.com/thought-leadership/summit-supercomputer/, accessed on May 2, 2019.

3. For more information on Ray Kurzweil go to http://www.kurzweiltech.com/aboutray.html, accessed on May 1, 2019.
4. From “Best Warren Buffet quotes, by topic” at https://25iq.com/quotations/warren-buffett/, accessed on May 9, 2019.
5. For detailed description of Modal logic see, *Stanford Encyclopaedia of Philosophy,* at https://plato.stanford.edu/entries/logic-modal/, accessed on May 22, 2019.
6. Richard H. Thaler, Cass R. Sustein, *Nudge*, Penguin Books 2009. For a detailed and interesting read on behaviour economics.
7. For further reading, go to https://policonomics.com/allais-paradox/, accessed on May 31, 2019.

Appendix C

RECOMMENDED STRUCTURE OF MINISTRY OF CYBERSPACE


MINISTRY OF CYBERSPACE
FINANCE DEPARTMENT
CYBERSPACE COORDINATION, HARMONISING AND RESOLUTION CENTRE (CHRC)
STATUTORY BODIES
INTERNATIONAL COOPERATION
INDUSTRY OUTREACH
AUTONOMOUS SOCIETIES, COMPANIES AND ATTACHED OFFICES
ICT COMPANIES
START UPS
CYBERSPACE INFRASTRUCTURE
WIRELESS
WIRED
DATA CENTER
OTHER SPECIALISED INFRASTRUCTURE
CYBER LEGISLATIONS AND POLICY
E GOVERNANCE
IndEA
DIGITAL DELIVERY OF SERVICES
R&D
HRD
RIGHT SKILL INDIA
EDUCATIONAL INSTITUTIONAL OUTREACH

Index

₹ 1280.00

KNOWLEDGE WORLD

KW PUBLISHERS PVT LTD

www.kwpub.com

ISBN 978-93-89137-47-7

9 789389 137477