



Credible Cyber Deterrence in Armed Forces of India



**Vivekananda
International Foundation**

Credible Cyber Deterrence in Armed Forces of India

“Nations must also take responsibility to ensure that the digital space does not become a playground for the dark forces of terrorism and radicalization”

- Prime Minister of India



**Vivekananda
International Foundation**

Published in March 2019 by
Vivekananda International Foundation
3, San Martin Marg, Chanakyapuri, New Delhi - 110021
Tel: +91-(0)11-24121764, +91-(0)11-24106698
Fax: +91-(0)11-43115450
E-mail: info@vifindia.org
Web: www.vifindia.org
Follow us on twitter@vifindia

Copyright © Vivekananda International Foundation

Design and production: <https://magnumcustompublishing.com>



“We are facing a future where security challenges will be less predictable; situations will evolve and change swiftly; and, technological changes will make responses more difficult to keep pace with. The threats may be known, but the enemy may be invisible. Domination of cyber space will become increasingly important... When we speak of Digital India, we would also like to see a Digital Armed Force.”

- PM's address to the Combined Commander's Conference, October, 2014

Table of Contents

Task Force Members	9
Foreword	11
Acknowledgements	13
List of Abbreviations	15
PART I	17
Executive Summary	19
Approach to Capacity Building	20
Seven Pillars for Capacity Building of Cyber Power: Indian Armed Forces	20
Note: FORMATION vis-à-vis Agency	21
Recommended Timelines and Roadmap	22
Recommended Missions of Cyber Formation	22
Recommendations	22
Policy: Cyber Warfare-enabled Armed Forces and Cyber Formation	23
Strategy for Cyber-enabled Armed Forces	24
Cyber Doctrine for Indian Armed Forces	25
Technology, R&D, Standards and Integrity of Data	28
Integration and Development of Concepts for Application of Cyber Power for effective Cyber Deterrence	29
International Engagement and Legal Framework	30
Priority Tasks of the Defence Cyber Agency (DCyA)	30
Organisation for Building Capabilities for Cyber Deterrence	32
Human Resource, Training and Certification	34
Recommended Approach for Technology Development	36
Contractual Clauses for System Protection and Availability	36
Emerging Threats and Negation Technologies	37
Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence	38

International Engagement and Legal Framework	39
Supporting National Institutions, Policies and Infrastructure	41
Policies and Infrastructure	41
Budgetary Assurance	42
Road Map and Action Plan	42
PART II	43
Section One: Policy and Strategy for Cyber Deterrence through Development of Cyber Power in Indian Armed Forces.	44
Environment Scan	45
The Indian Scene	47
Approach to Capacity Building	48
Seven Essential Factors Constituting Cyber Power	49
Seven Pillars for Capacity Building	50
Note: FORMATION vis-à-vis Agency	51
Section Two: Policy and Strategy for Developing Cyber Capability of the Indian Armed Forces	52
Introduction	53
Aim	53
Threat Scenario	53
Characteristics of Cyber Warfare	54
Military Targets for Cyber Warfare	55
Role of Cyber Formation/Defence Cyber Agency	55
Policy for Creating Cyber Warfare Enabled Armed Forces	56
Strategy	57
Conclusion	58
Section Three: Indian Armed Forces Doctrine for Application of Cyber Power and Information Operations	59
Indian Armed Forces Cyber Doctrine	61
Organisation and Adaptation of Cyber Force	62
Human Resource, Training and Certification	63
Technology, R&D, Standards and Integrity of Data	65

Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence	67
International Engagement and Legal Framework	68
Section Four: Organisation for Cyber Deterrence, Synergy, Staffing and Adaptation of Cyber Force	69
Organisation for Capacity Building in Cyber Deterrence	71
Section Five: Human Resource, Training and Certification	77
Focus Area of Securing Military Cyber Space	79
Some Other Issues	81
Conclusion	82
Section Six: Technology, R&D, Standards and Integrity of Data	83
Introduction	84
Suggested Approach for Technology Development	84
Emerging Threats and Corresponding Negation Technologies	86
Priority Technologies for Defence Forces	86
Research and Development	90
Contractual Clauses for System Protection and Availability	91
Contract Goals	92
Conclusion	92
Section Seven: Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence	93
Synergy, Jointness and Integration	96
Development of Concepts for Application of Cyber Power	96
Section Eight: International Engagement and Legal Framework	97
International Engagement	98
Military Diplomacy	102
Legal Framework	103
Introduction	104
The Constitution of India and Cyber War	104
Cyber Space Jurisdiction	105
Rule 2 of Tallinn Manual	105

Establish Nation-wide Cyberwar fighting Processes and Procedures	106
Privacy and Cyberwar	106
Cyberwar and Deniability	107
Protection to the Engaging Forces	107
Amendment to Section 69 of the Information Technology Act	108
Conventions and Treaties	109
Cyber Forensics	110
Rules of Engagement	110
Some Actions/Matters which may be Acceptable as the Rules of Cyber Engagement	111
Role of Defence Services Headquarters	111
State of Cyber Readiness	111
Preparedness by Defence Forces	111
Recommendations and Timelines	112
Section Nine: Supporting Institutions, Policies and Infrastructure	113
Establish National Cybersecurity Commission (NCSC)	114
Cyber Policy Research Centre	114
Integrated Cyber Threat Intelligence Centre	115
Indian Cyber security Operations Centre	115
Assurance Framework, Test and Certification	115
An Agency for Information Security	115
National Centre for Cybersecurity Resilience	115
Cyber Command.	115
National Policies to be Revised and Infrastructure	116
Section Ten: Comprehensive Cyber Power at National Level	117
Recommended Integration of DCyA at National Level	119
Section Eleven: Road Map and Action Plan	122
Invited Experts	124
Task Force Team	126

Task Force Members

1. Lt. Gen. Davinder Kumar, PVSM, VSM Bar, ADC (Veteran)
2. Lt. Gen. Anil Kumar Ahuja, PVSM, UYSM, AVSM, SM, VSM & Bar (Veteran)
3. Lt. Gen. (Dr.) V.K. Saxena, PVSM, AVSM, VSM (Veteran)
4. Lt. Gen. (Dr.) S.P. Kochhar, AVSM Bar, SM, VSM, ADC (Veteran)
5. Maj. Gen. P.K. Mallick VSM (Veteran)
6. Brigadier Abhimanyu Ghosh (Veteran)
7. Brigadier (Dr.) Ashok Kumar Pathak (Veteran)
8. Commander Arun Saigal (Veteran)
9. Commander Mukesh Saini (Veteran)
10. Air Commodore Devesh Vatsa VSM

Foreword



उसको क्या जो दंतहीन, विषरहित, विनीत, सरल हो
सहनशीलता, क्षमा, दया को, तभी पूजता जग है
बल का दर्प चमकता उसके पीछे जब जगमग है!

-रामधारी सिंह दिनकर

India has to be militarily powerful to be a meaningful player in international politics. As the world's fifth largest economy, it must be a secure nation to deter her enemies. India's Poet Laureate Dr. Ramdhari Singh Dinkar, in his poem quoted above, has correctly observed that only the powerful possess the ability to pardon someone and that no one cares for the weak or toothless.


Cyber strategies and deterrence are the new 'normal' of national power. Historically speaking, the doctrinal response to new strategic challenges has always been slow and reactive. For example, it took a year to respond to submarine warfare (1914); almost two decades to evolve a doctrine against strategic air bombing (1937); a half-a-decade passed before mechanised warfare (1940) evolved to counter mechanised forces; the doctrine of nuclear deterrence took many decades to evolve after the first use of a nuclear bomb in 1945. Global powers are still struggling to evolve ways to counter cyber warfare. Addressing the Combined Commanders Conference in October 2014, Prime Minister Modi said, 'When we speak of Digital India, we would also like to see a Digital Armed Forces'.

Aware of cyber power being a critical component of India's comprehensive deterrence capability, the Vivekananda International Foundation set up a task force under the chairmanship of Lt. Gen. Davinder Kumar (Retired) to suggest a road map for cyber deterrence in her armed forces. I am happy to present the task force's report for discussion and debate.

The task force has primarily concentrated on military aspects of cyber deterrence and how it should be integrated with national capabilities. It has made recommendations in policy, strategy, organisation, technology, manpower, international engagement, legal framework, research and development, and training. A fair attempt has been made to look at it from a higher perspective where cyber war becomes a subset of cyber power. The report identifies seven pillars for enhancing the cyber capabilities of the Indian armed forces, including operationalisation of a 'Defence Cyber Agency' as a stepping stone to develop cyber power within the designated time frame.

Lt. Gen. Davinder Kumar (Retired) was the Signals Officer-in-Chief of the Indian Army and after retirement has devoted himself to the study and analysis of cyber issues, and particularly the emergence of India as a cyber power. The other members of the task force looked at development and application of cyber power as a means of conveying cyber deterrence. I would like to thank Lt. Gen. Kumar and his team for their painstaking research, focused approach and sincerity in preparing this report. My special thanks to all invited experts for their contributions in making this report.

New Delhi
27 March 2019



Dr. Arvind Gupta
Director, VIF

Acknowledgements

At the very outset, I would like to convey my grateful thanks to Dr. Arvind Gupta, Director, Vivekananda International Foundation (VIF) and Lt. Gen. Ravi Sawhney PVSM, AVSM (Veteran), Centre Head and Senior Fellow, for assigning this subject for study, providing necessary guidance, support and a balanced and highly experienced team to prepare this report. It is rare to have a task force with over 400 years of collective wisdom and varied experience, both in combat and policy making. Each member of the task force made a sizable contribution and I would like to express my gratitude for their contribution to the task assigned and for their participation in stimulating informed discussions in a frank and forthright manner. Resultantly, we have an India-centric comprehensive document dealing with all aspects of acquisition and application of cyber power in line with recommended policy, strategy and doctrine. The task force is confident that implementation of these recommendations would fill a strategic gap in India's security architecture and provide the base for the creation of a Cyber Command.

My grateful thanks to Ms. Anuttama Ganguly, Joint Secretary, and her team for providing excellent logistic support. Our thanks also to the IT, editing and printing teams.

My special thanks to the 'Invited Experts', who so willingly gave their time and valuable inputs. My grateful thanks to Member Secretary Commander Mukesh Saini for his excellent time management in facilitating realtime information sharing amongst members and assistance in creating the final document, besides working on the legal framework.

Finally, I reiterate that the team worked diligently in 'mission' mode and delivered on schedule. I could not have asked for anything more.

Lt. Gen. Davinder Kumar, PVSM, VSM Bar, ADC (Veteran)
Chair Person, Task Force

List of Abbreviations

AoR	Area of Responsibility
BREXIT	Britain to exit the European Union
CAN	Computer Network Attack
CBMs	Confidence Building Measures
CC-TLD	Country Code Top Level Domain Servers
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CISO	Chief Information Security Office
CIWO	Command Information Warfare Officer
CND	Computer Network Defence
CNO	Computer Network Operations
CSO	Cybersecurity Officer
DASI	Directorate of Air Staff Inspection
DCyA	Defence Cyber Agency
DDoS	Distributed Denial of Service
DevSecOps	Development - Security - Operations
DGND	Director General of Naval Design
DIARA	Defence Information Assurance and Research Agency
DLP	Data loss prevention
EDR	Endpoint detection and response
ELINT	Electronic Intelligence
EM	Electro- Magnetic
EW	Electronic Warfare
GCHQ	Government Communications Headquarters
HPC	High-performance computing
HUMINT	Human Intelligence
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IEW	Information and Electronic warfare
IMO	International Maritime Organisation
IoT	Internet of Things
IT Act, 2000	Information Technology Act 2000
ITU	International Telecommunication Union
IW	Information Warfare
MASINT	Measurement and signature intelligence

MDR	Managed detection and response
MeitY	Ministry of Electronics and Information Technology
MiM	Man-in-the-Middle
NCC	National Cadet Corp
NCCC	National Cyber Coordination Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NCSC	National Cyber Security Commission
NCSP	National Cybersecurity Policy
NEP	National Electronic Policy – 2012
NIB	National Information Board
NMCOC	National Maritime Cyber Operations Centre
NSCS	National Security Council Secretariat
NSQF	National Skill Qualification Framework
NSS	National Service Scheme
NTA	Network traffic analysis
NTRO	National Technical Research Organisation
OPSEC	Operational Security
OSCE	Organisation for Security and Cooperation in Europe
OSINT	Open Source Intelligence
OSS	Operational Support System
QRT	Quick Response Team
RoCyE	Rules of Cyber Engagement
SaaS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SCO	Shanghai Cooperation Organisation
SIEM	Security Information and Event Management
SIGINT	Signal Intelligence
SOC	Security Operation Centre
TA	Territorial Army
TLD	Top Level Domain
UBA	User-behaviour analytics
UNGGE	United Nations Groups of Governmental Experts
VAPT	Vulnerability Assessment & Penetration Testing
VDN	Virtual Dispersive Networking
WESEE	Weapons and Electronics Systems Engineering Establishment
WMD	Weapon of Mass Destruction
WSIS	World Summit on Informational Society

PART I

Executive Summary

Military practitioners have been excited by the use of the term 'cyber war' for some years now. Influence of technology on warfare is increasing, and cyber capabilities only emphasise the fact. It is often mooted that information technology and cyber could well determine the victor in the digital battlefield of tomorrow.

Twenty-first century warfare is all about improved situational awareness, contextual knowledge, discerning disposition and synergised action. Technological breakthroughs have profoundly altered and shaped the doctrinal, organisational and strategic contours of warfare. Information Technologies, sensors, miniaturisation and ubiquitous wireless connectivity have created an entirely new domain of warfare by way of 'cyber space' and put warfare on the cusp of an epochal shift from the conventional to an information-based virtual age. This wave of cyber-driven transformation is radical, sweeping and innovative, demanding a relook at established strategic plans and to chalk out a new direction for operational enhancement and improved tactical efficiency. Cyberspace and cyber power offer a whole new set of technological solutions to some of the challenges of modern warfare.

Cyberspace promises distinct advantages in a connected world, from intelligence accretion and analysis to faster and more reasoned decision-making. As we become

more and more reliant on cyber power, vulnerability also increases and proper safeguards are absolutely essential. It is certain that complexities in this form of conflict will increase and so will their impact. It behoves us therefore, to recognise the need for developing cyber power by way of skilled human resource, formal training, technology, research and development, and necessary funding. Application of cyber power must form part of our planning process.

Though instruments of cyber power can work independently, there is an exponential increase in their effects when deployed with Electronic Warfare (EW) and Kinetic Energy systems. Cyber power application will have a significant impact on other warfare domains. One may state that in times to come, 'cyber superiority' will be an essential and operational imperative.

Developments of cyber power for offensive operations in cyberspace significantly expand options available to policymakers and field commanders.

The consequences of the application of cyber power for offensive operations may vary in severity, lethality, intent or geographical distribution and can manifest in complex, dynamic and unpredictable ways, having far-reaching tactical and strategic implications.

We need to formulate and promulgate our policy for capacity building of cyber

deterrence related strategy, and a doctrine for our armed forces. Accordingly, the task force set its aim as follows:

TO PREPARE A ROADMAP AND AN ASSOCIATED ACTION PLAN FOR ACQUIRING CREDIBLE CYBER DETERRENCE ACROSS FULL SPECTRUM IN THE ARMED FORCES, COMMENSURATE WITH INDIA'S STANDING AND SECURITY NEEDS AND INTEGRATING THE SAME WITH THE NATIONAL CYBER SECURITY ECO-SYSTEM.

Approach to Capacity Building

India released its National Cybersecurity Policy (NCSP) in 2013. This very comprehensive document deals with almost all facets of cyber security. Surprisingly, NCSP-2013 does not talk about the creation and application of cyber power; the role, organisation, equipping and training of the Indian Armed Forces to execute cyber-enabled operations and cyberwar; leaving a glaring gap in national security.

There is an urgent requirement to enunciate our national cyber power policy and doctrine, build 'Cyber Power as a System' commensurate with India's security needs and integrate it with other warfighting domains to guard against the full spectrum of threats.

The government, very recently, has accorded approval for the raising of a Defence Cyber Agency (DCyA). It is felt that at best, this is a half-hearted attempt, keeping in mind the threats and India's geopolitical role.

The task force recommends that the formation of DCyA be taken as an intermediate step towards the formation of a full-fledged Cyber Formation or Cyber Command over the

next three years and concurrently develop capabilities for full spectrum Information Warfare with cyber power as one of its major constituents.

The task force accordingly decided it would follow two approaches – one that would concentrate on capability build up within our armed forces, and secondly, a suggested integration with the national cybersecurity architecture at a macro level.

The task force recommends building of credible cyber deterrence through development of capabilities for cyber power for our armed forces on the **Seven Pillars** illustrated below:

Seven Pillars for Capacity Building of Cyber Power: Indian Armed Forces

1. Policy and Strategy for Development and Employment of Cyber Power
2. Indian Armed Forces Doctrine for Application of Cyber Power and Information Operations
3. Organisation for Cyber Deterrence, Synergy, Staffing and Adaptation of Cyber Force
4. Human Resource, Training and Certification
5. Technology, R&D, Standards and Integrity of Data
6. Integration and Development of Concepts for Application of Cyber Power for effective Cyber Deterrence
7. International Engagement and Legal Framework

Note: FORMATION vis-à-vis Agency

A 'Formation' is an organisation entity in the Indian Army like a Brigade, Division, Corps and Command. There is no organisation like an 'Agency'. The raising of a Defence Cyber Agency is perhaps the lowest in the rung, not well understood, has limited resources and would not be in a position to convey 'Deterrence' as stated in the recommended Cyber Doctrine for the Indian Armed Forces.

Accordingly, the task force felt that while a Defence Cyber Agency is a long awaited and a welcome measure, it must provide the base for an Indian Cyber Command which must be created within the next three years to effectively respond to likely and emerging threats.

Since one is not certain of the government's likely decision, the report has expressions like 'Formation/DCyA'. Formation conveys the organisational level of cyber power, (cyber brigade/division/corps/command) is a familiar entity, and hence, well understood. Recommendations made in the report are equally valid to both, the Formation and Defence Cyber Agency.

Further, the terms convey the long-term applicability and validity of the report as the DCyA transforms to a Cyber Command.

Recommendations

Formation of Defence Cyber Agency (DCyA) be taken as an intermediate step towards the formation of a full-fledged Cyber Formation or Cyber Command over the next three years, while concurrently developing capabilities for full spectrum Information Warfare with cyber power as one of its major constituents.

Build capabilities of cyber power for our armed forces on **Seven Pillars** as illustrated below:

1. Policy and strategy for development and employment of cyber power
2. Indian Armed Forces doctrine for application of cyber power and information operations
3. Organisation for cyber deterrence, synergy, staffing and adaptation of cyber force
4. Human resource, training and certification
5. Technology, R&D, standards and integrity of data
6. Integration and development of concepts for application of cyber power for effective cyber deterrence
7. International engagement and legal framework

Recommended Timelines and Roadmap

The suggested timelines and associated recommendations are mentioned. Most activities have to start concurrently. Following legends have been used:

- {Immediate} – Action on these recommendations should start with utmost urgency and should be completed within six months of approval of recommendations
- {Priority One} – These recommendations should not take more than one year to complete
- {Priority Two} – These recommendations are not necessarily of lesser priority but expected to take up to two years
- {Priority Three} – Work on these recommendations is contingent on completion of some other recommendations or require elaborate execution. However, implementation should not take more than three years

Recommended Missions of Cyber Formation are:

- Defending own computer networks, platforms and weapon systems
- Defence against foreign-origin or foreign-sponsored cyberattacks,

especially if they cause loss of life, property or significant foreign policy and economic consequences

- Provide offensive cyber options, to be implemented on approval as force multipliers for other operations. This would include covert operations
- Synergising cyber intelligence with Signals Intelligence, Electronic Intelligence (ELINT), Human Intelligence (HUMINT) and operational security for a comprehensive threat analysis in the information warfare domain
- Plan and execute cyber deception
- Recruit, train, retain and periodically refresh human resource. Equip them and be responsible for their cadre management
- Be a part of 'Military Diplomacy' and exchange information with friendly nations, joint training and follow an integrated approach for Internet governance, legal framework and favourable policies
- Effectively liaison with civilian counterparts for policy making, processes, exchange of information, and ensure interoperability of systems
- Establish a suitable organisation for information assurance and management
- Create necessary 'Systems' and infrastructure for training, laying down of policies and processes
- Establish technology research facilities, both by the Services and jointly with the private sector

- Ensure budgetary support and effective liaison with other agencies, academia and R&D establishments

Policy: Cyber Warfare-enabled Armed Forces and Cyber Formation

- Provide a dedicated, trained and equipped military organisation to execute all operational aspects in this domain
- Cyber Formation/DCyA would work in conjunction with the overall national Cybersecurity architecture, including the three Services
- Be responsible for conduct of 'cyber support operations' to include:
 - intelligence collection, collation, analysis and dissemination
 - Cyber deterrence
 - Formulation of prioritised cyber target lists of potential adversaries
 - Plan and execute retaliatory offensive operations
 - Conduct testing and certification of hardware and software
 - Assist in development of indigenous technologies, weapons, cryptology and cryptoanalysis tools and language
 - Conduct training and cyber exercises, and management of international cyber cooperation

Cyber Formation /DCyA to have a robust legal component to ensure operations are conducted in compliance with the rules of engagement, international and domestic laws, and that enough legal justification exists

for transcending to physical conflict (kinetic offensive action) when necessary.

The Cyber Formation would be responsible for planning and conducting of cyber offensive operations, deception and cyber exploitation, particularly related to likely targets, vulnerability assessment, probing missions, penetration testing and exploitation of adversary networks.

It would also be responsible for complete information management and information assurance.

Strategy for Cyber-enabled Armed Forces

- Creation of an appropriately 'situated and constituted' operational formation for all aspects of cyber power to convey deterrence across full spectrum (Immediate)
- The primary responsibility for cyber defence would rest with respective ministries, departments, organisations and industry
- Services (Army, Navy and Air Force) would be responsible for their basic cyber security, to include cyber resilience and defence in depth Cyber Command/Formation would be responsible for specific military aspects and be the only organisation authorised, equipped and trained to conduct offensive cyber operations, including those related to strategic intelligence and deception
- Cyber Formation would be responsible for enforcing compliance of policies enunciated by the National

Cybersecurity Organisation. It would be responsible for testing and validating all software and hardware to be used, particularly in critical areas; setting up a facility for examining and certifying all hardware procured/manufactured, and participate in all decisions/discussions related to the award of contracts or projects {Priority One}

- Formulate robust 'rules of engagement' for responding to cyber attacks and authorise the cyber command or formation for the conduct of such operations
- Formulate contingency plans for 'Degraded Operations', evolve and rehearse continued execution of operations in different spheres, albeit with degraded capability
- Cyber Command/Formation to be responsible for creating superior military capabilities in cyberspace
- Cyber Formation to be responsible for simulator training and for setting up and managing the National Cyber Range
- Cyber Command/Formation to be structured and empowered to outsource operations and employ embodied personnel selectively
- Cyber Command/Formation to be responsible for evolving a 'Cyber Technology Perspective and Capability Road Map' for Information Warfare

Cyber Doctrine for Indian Armed Forces

India must release at the earliest an 'Integrated National Cyber Doctrine', developed jointly by the civil authority and the armed forces with 'Cyber Security' dealt by the civil authorities and 'Cyber Power' by the armed forces. {Priority One}

The application of cyber power, either on its own or in conjunction with other constituents of power, should be decided by the Cabinet Committee on Security (CCS), keeping in mind the overall threat scenario, the impact on national security and the responses needed for a given situation.

The following situations would warrant application of cyber power either by itself or integrated with other instruments of power:

- Any cyber intervention which adversely impacts:
 - India's sovereignty and security
 - Availability of India's critical information infrastructure
 - Free navigation, mobility and freedom of action in the electromagnetic and cyber space of India
- Any cyber probing mission resulting in loss of a platform, manned or autonomous, will be considered as an act of war and would attract response accordingly
- Exfiltration of sensitive information having an adverse effect on the economy, financial system, defence, security, atomic infrastructure and strategic industry would draw a strong and focused response in any manner India deems fit.

For the purpose of cyber deterrence and application of cyber power, both civil and military assets would be considered as one. However, subsequent to clearance by the nominated authority, the conduct of a cyber offensive or cyber deception would be the prerogative of the armed forces.

Indian Armed Forces cyber doctrine would be

Multi-layered resilience with active defence and deterrence

This doctrine would form the basis for developing full spectrum of cyber power in the armed forces which would comprise of cyber-crime investigation including cyber forensic, counter cyber terror operations, cyber espionage, and in-depth cyber defence with particular emphasis on platforms, cyber offensive, cyber deception, cyber-enabled operations and cyberwar either by itself, or in conjunction with EW and kinetic means.

Development of processes and capabilities for employing cyber power in different operations and training of cyber leaders must be top priority.

While the responsibilities of the civil authorities and armed forces must be unambiguously defined, the absolute necessity of information exchange, integration of capabilities, joint training and development of mission-oriented cyber weapons, and so on, should also be clearly emphasised.

A dedicated organisation tasked with the raising and operationalisation of 'Defence Cyber Agency' (DCyA), suitably empowered and with assured budgetary support, would be central to building requisite capabilities. {Immediate}

Implementation would be done in two parts concurrently and monitored by the Chiefs of Staff Committee periodically:

- Part 1, enhance the capabilities of each Service and raise DCyA as an umbrella organisation responsible for training, equipping, fielding, infrastructure, integration and information management
- Part 2, integration of cyber power with cybersecurity architecture at the macro level and command and control ensuring least turbulence in implementation and be flexible enough to face new threats and accept new technologies

The country needs to build a thought leadership and weave together India's potential to create cyber deterrence under one organisation with complete responsibility, accountability and budgetary support

The exercise of cyber power is entirely dependent upon the tactical skills of the operator as he is the 'man behind the gun'. At the operational and strategic levels, we need cyber leaders to plan and conduct cyber operations, both in stand-alone and integrated applications, in conjunction with IW and kinetic power.

Innovation, change of working culture, attractive provisions with regard to pay and allowances, creation of an appropriate cadre with multiple avenues for growth and promotion, recognition and status backed by concentrated training, acquisition of skills and chance of location across the globe are a few measures which may help in getting and retaining the right human resource.

The armed forces must ensure near 100 percent computer literacy over the next three years which must include 'Good Practices' and 'Cyber Hygiene' to be followed by all. Computer awareness, literacy and aptitude must be reflected in the appraisal which could form the basis of retraining and selection of cyber warriors. {Priority One to Three}

Availability of cyber warriors and cyber leaders across multiple skills which constitutes cyber power is an extremely critical factor and perhaps the biggest challenge. The armed forces will have to adopt a multi-level approach and concurrent execution. Following may be considered:

- Establish world-class training facilities along with industry and academia to impart training with curricula for different levels and highly qualified faculty. {Priority One to Two}
- Select/Recruit younger jawans/sailors/airmen with necessary qualifications and aptitude for ICT and computers and train for three to four months to concentrate on Computer Network Defence (CND). The brightest amongst these should be listed for Computer Network Attack (CNA) training after a tenure of two years in the field. This training could be outsourced to corporate or academic establishments on a zonal or a region basis {Priority One to Three}
- While we must exercise the option of outsourcing, the armed forces must have their own military training facilities and system integration with IW and KE assets {Priority One to Three}

- Select M.Tech.-qualified officers and send them to countries like Israel, UK, USA, South Korea and Russia for training in cyber warfare, participation in field exercises, and learn processes and drills for employment of cyber power in the Indian context. These officers will form the nucleus in accordance with the concept of 'Train the Trainers'. They will also form the backbone of the cyber leadership {Priority One}
- Multi-level cybersecurity should be introduced as a topic for graduate, post-graduate and doctoral studies in Indian institutions {Priority Two}
- Special care and emphasis on selecting people for Computer Network Exploitation (CNE). They must be trained specifically in different languages, information assurance, big data, analytics, co-relation, Artificial Intelligence, cryptanalysis, code breaking, blockchain, analysis of 'kill switches', patch management, network management systems and designing of both disruptive and destructive cyber weapons {Priority One to Three}
- Emphasis must be on correct recruitment, training, retention and re-training. Rules must be flexible and focused on attracting the requisite resource. Some degree of relaxation in regimentation and working environment would be in order
- An extremely important aspect of training would be the development of an offensive spirit, agility of mind and mental robustness to withstand cognitive attacks aimed at behavioural change, perception management and lowering of morale {Priority One to Three}
- Explore organisations like the National Cadet Corps (NCC), National Service Scheme (NSS) and police cadets to provide young, motivated and disciplined resource for the cyber warrior cadre. All these organisations must have cyber wings which act as a nursery to meet the requirements of cyber operators and warriors partially {Priority One to Three}
- Raise at least one Territorial Regiment in each Command capable of conducting all types of cyber operations, particularly CND and counter-offensive and detaching integrated teams in support of operations {Priority One to Three}
- The launch of a cyber offensive or cyber deception would be the responsibility of the cyber formation. Accordingly, at least 10 integrated teams will be created in three years on an incremental basis {Priority One to Three}
- As part of 'Crowd Sourcing', create an organisation like 'Institute of Cybersecurity Professionals', select highly qualified resource from corporate, academia and R&D establishments to be 'on call' to assist during crises. Initially, they could be invited to contribute in the formulation of strategy and assist in the capability build up {Priority One to Three}

- Involve Indian diaspora for technology, training, investments and setting up R&D facilities {Priority One to Three}
- The armed forces must immediately establish an 'Academy of Information Operations and Management' with dedicated wings and facilities for training in the employment of cyber power across the full spectrum. This must be independent of the training facilities of the Services and must concentrate on advance training and strategy with the requisite participation of the civil sector {Priority One to Three}

Technology, R&D, Standards and Integrity of Data

Analyse and revise the National Electronic Policy (NEP) – 2012 under the 'Make in India' programme to meet the requirements of both cybersecurity and cyber power. It must be made more attractive for people to invest. {Priority One to Three}

The policy must concentrate on production of secure products and systems, their integration with expertise in 'engineering to production' based on Indian standards for information security and secure products which are about to be released. Special emphasis must be put on the design and availability of 'secure industrial control systems'.

Given that semiconductor chip manufacturing foundries are capital intensive with still longer gestation periods, it may be a good idea to hire facilities abroad initially. This would compress the time frame for the development of skills and be cost-effective, while concurrently, we establish our own

facilities. This approach would mitigate the risk to supply chain vulnerabilities to a large extent, especially in the case of critical systems. {Priority One to Three}

India being one of the fastest growing Internet and smartphone markets carries substantial clout. She must use that for getting favourable terms with regard to the integrity of chips, ensure a supplier's responsibility in case of malware, cyber insurance and fastest delivery of patches/kill switches, with a penalty for delays. Joint inspection facilities for chips, products and systems must also be considered. These should be an integral part of the contract document and would be easier to incorporate if manufacturing is being done in India. {Priority One to Three}

Encourage start-ups and small and medium-sized enterprises (SMEs) to work on secure software, products and systems. Some have done well, exported their products and established joint ventures. Military orientation should be relatively easy and must be explored. {Priority One to Three}

A formal military-industry interface and their association with design and manufacturing agencies is necessary. {Priority One}

We must have an organisation like the Weapons and Electronics Systems Engineering Establishment (WESEE) in all three services to start with and later establish the same in selected commands. {Priority One}

Integrated teams must carry out a regular audit of platforms, weapons, systems and software to find vulnerabilities and how to close those. The manufacturer must be made equal partner through well-drawn contract and

be responsible for 'availability' of systems, regular inspection to look for malware and release of patches to nullify any vulnerability or accommodate the change in technology. {Priority One to Three}

Consider appointment of an Inspector General (Cybersecurity) to be assisted by a small team of experts like DASI of the Indian Air Force, to oversee cybersecurity of platforms and weapon systems during peace and field exercises. {Priority Two}

R&D for product development and cyber weapons: India needs focused R&D in the development of safe products, discovery and analysis of vulnerabilities, fixing attribution, the design of 'kill switches' and security patches; creation and analysis of malware, production and delivery of cyber weapons and concentrate in capability building for electronic combat as part of Information Warfare (IW). {Priority One}

The Indian Armed Forces must have modern means and capabilities for cyber exploitation, technical intelligence, cyber deception and launching of probing operations. In addition, depending on the knowledge of vulnerabilities, it must develop cyber weapons, both for causing disruption and destruction. {Priority One to Three}

Sharing of intelligence between the civil and military as also the launch of cyber weapons are a must and should be ensured through a statute if necessary. {Immediate}

Ensuring correctness of information and integrity of data are absolutely critical requirements along with regular surveillance for any 'Insider Threat' for sabotage, stealing technology or exfiltration of data.

Continuously examine options and devise a methodology for the acquisition of technology to include R&D, manufacturing, and availability of human resource with requisite skills and requirements of infrastructure like cyber range, networks for simulation, and for making of cyber weapons. {Priority One to Three}

Integration and Development of Concepts for Application of Cyber Power for effective Cyber Deterrence

The foremost task of the Cyber Formation/DCyA would be to ensure that integration is embodied across all functions, including operations, intelligence, technology management, perspective plans, logistics and human resources development (HRD). Such embodiment enables common understanding leading to efficient and optimised responses.

Cyber Formation/DCyA would also jointly formulate processes for collaboration with the diplomatic, economic and information instruments of the national power, at all levels – strategic, operational and tactical. {Priority Two}

An integrated approach comprising of proactive engagement and shared understanding would be developed to bring distinct professional, technical and cultural disciplines of entities and sub-entities together. {Priority Two to Three}

Capacity building of cyber power would depend on appropriate mission sets, targets and spheres of operation. Based on these, the armed forces will work out tactics, techniques, procedures and authorities in cyberspace for military operations.

While cyber logistics has emerged as a new field requiring expertise and attention, cyber deception is an essential capability both for cyber defence and cyber warfare.

‘Electronic Combat’ with integration of computer network operations (CNO), electronic warfare (EW) and electromagnetic spectrum (EM Spectrum) has taken Information Warfare (IW) to a new level and has provided unique capability focused on the exploitation of asymmetry.

International Engagement and Legal Framework

While India has signed several bilateral, regional and multilateral agreements for cooperation in cyberspace, special efforts would be required for armed forces training, participation in exercises, military diplomacy, sharing of information of military value, joint development of technology and a common voice in the formulation of laws and policies. Such agreements with friendly countries can improve capacity building and must be given impetus at the highest level. The positioning of cyber experts in our diplomatic missions abroad is strongly recommended. {Priority One to Three}

The armed forces must have forensic resources to investigate cyber-crimes effectively. These could be add-on resources in the legal department of the Services. Leaders must be conversant with the IT Act 2000 as amended in 2008. They also should be aware of the organisation for Internet Governance, ICANN, Tallinn Manuals and UN laws/deliberations of cyber war and cyber interventions. {Priority Two to Three}

Priority Tasks of the Defence Cyber Agency (DCyA)

The first and foremost task of the Cyber Formation/DCyA would be to release a policy document detailing the cyber power eco-system for the armed forces, capacity building in each Service, and integration at DCyA headquarters. {Priority One}

The DCyA would coordinate and issue necessary policies, ensure the creation of suitably empowered and integrated organisations on the ground, facilitate release of funds, ensure availability of skilled manpower and training infrastructure. {Priority One to Three}

These organisations must have government sanction to facilitate development of cyber logistics and infrastructure for training, establishments of laboratories and release of funds. {Priority One}

Based on policies and processes promulgated by the Cyber Formation/DCyA, each Service must provide resources, manpower, basic training, infrastructure, and logistics for capacity building to ensure necessary defence and resilience against envisaged threats. {Priority One to Three}

Create awareness about cyber threats in all ranks of the armed forces, their impact in all areas of our existence and the ability of cyber weapons to cause disruption and destruction almost equivalent to weapons of mass destruction (WMD). {Priority One to Three}

Commanders to be sensitised to digital domain threats, operations as part of the Information Warfare in a digitised battlefield and the certainty of an adversary

launching cyber weapons, cyber deception and 24/7 monitoring of our networks and communication systems as part of cyber intelligence, besides conducting cyber-enabled operations with kinetic power. They must overcome complexes with regard to cyber power being 'technical' and concentrate on developing its application, both for cyber resilience and cyber offensive. {Priority One to Three}

Formation and unit commanders/ equivalent must ensure that the work and responsibilities of cyber personnel are given due importance and recognition and that they are treated with professional dignity at par with other fighters. {Priority One to Three}

Each Service must ensure availability of cyber qualified resources at the unit/ ship/squadron level under a nominated Cybersecurity Officer/Chief Information Security Office (CSO/CISO)), chartered with the responsibility of training, creating general awareness, information assurance, regular monitoring of possible threats, readiness of the establishment for cyber resilience measures and ensuring that activities as part of cyber hygiene and good practices are in order and complied with at all levels. {Priority One}

Special attention must be given to the use of social media and look out for any 'insider threat' during the periodic but random audits. Surprise audits and checks must be instituted and to be conducted by empowered teams from the respective Service Headquarters/ DCyA. {Priority One to Three}

Cyber formation/DCyA must formulate parameters for measuring the 'Cybersecurity Index' (CSI) of a unit/organisation and communicate the same to all concerned.

Measurement of CSI will be a part of the annual inspection of the establishment. A score below the required threshold will invite special measures by the DCyA. {Priority Two to Three}

Each Service Headquarters will ensure that necessary training and infrastructure is available for the men to prepare for Certification Tests to be conducted by DCyA or other nominated agency {Priority One to Three}

Cross-domain training and exercises involving persons from each Service and DCyA must be done regularly. Actions to obviate the flaws particularly related to the discovery of vulnerabilities must be undertaken on top priority and a record maintained. All concerned must be informed and that data be maintained at the nominated data centre to ensure integrity. {Priority Two to Three}

There is a strategic, inescapable and urgent requirement for a 'Directorate of Information Assurance and Management' at the tri-service level with its nodes at each formation/equivalent connected with each other and further with the data centres established by each Service. {Priority Two to Three}

Institute a Cyber Cadre with immediate effect with flexible construct and less regimentation. {Immediate}

As part of intelligence acquisition and monitoring, recruit requisite resource to operate in the dark web and deep web and monitor it. This capability and task could be given to the Defence Intelligence Agency (DIA) and coordinated with the National Intelligence Agency (NIA) at the appropriate level. {Priority Two to Three}

Recruit, train and deploy 'cyber modules' and 'lone wolf' operators for strategic intelligence and special tasks. {Priority Two to Three}

Organisation for Building Capabilities for Cyber Deterrence

Indian Army

The army must be organised, equipped and trained for Information Warfare and must have integral capabilities to thwart electronic/cyber interventions, launch offensive operations at the tactical level and provide a launch pad to DCyA teams for offensive operations (CNO). {Priority One to Three}

The Indian Army needs to balance its obsession with kinetic energy systems with the absolute necessity of ways and means for 'Electronic Combat' (IW+EW+EM Space) for that is the most likely threat which manifests 24/7. {Priority One to Three}

Measures for ensuring computer network defence (CND) should be available at all levels of command and integrated cyber, IO and EW organisation at the formation level. Information Warfare brigades with specialised units in the cyber domain, EW and IO should be on the 'Order of Battle' of a Corps to begin with. {Priority One to Three}

The Directorate General of Information Systems be transformed to a Tri-service Directorate of Information Security and provide the secretariat for 'Cybersecurity Advisory Committee' at Headquarters IDS. {Priority Two}

Indian Navy

The Indian Navy would have overall responsibility for maritime cyber defence and to provide a firm base for cyber offensive operations to the DCyA.

An empowered coast guard to be responsible for cyber defence of all shore establishments and to conduct periodic audit of compliance with DCyA and Naval Headquarter's policies and processes.

The Cyber Formation or Defence Cyber Agency to oversee all aspects of cyber power capacity building across the maritime domain in coordination with institutions like National Security Council Secretariat (NSCS), Computer Emergency Response Team (CERT), National Technical Research Organisation (NTRO) and National Critical Information Infrastructure Protection Centre (NCIIPC).

The National Maritime Cyber Operations Centre (NMCOC) would be the coordination centre for cyber operations within the Navy, Coast Guard and other services. The CERT-Navy and its Cyber QRTs would be part of it.

The WESEE would be the nodal technical cyber advisor to develop a cyber-secure framework, including for Internet of Things (IoT) and to issue relevant guidelines for implementation and inspection of cybersecure naval equipment, including naval propulsion and engine control systems. {Priority One to Three}

WESEE would guide Director General of Naval Design (DGND) on design, inspection, development, manufacture, installation of connected onboard sensors and weapons of all naval vessels i.e., from design to delivery

and subsequent operationalisation. {Priority One to Three}

Shipboard Cyber Expertise: While the Navy must have a dedicated Chief Information Security Officer on board, as an interim measure, the skill set of the officer looking after communications and EW needs to be enhanced to include all aspects of cybersecurity and application of cyber power. {Priority One to Three}

Integral establishments of the Navy like the Signal School, INS Valsura and the Submarine and Naval Aviation Training School should be organised and equipped for military training in application of cyber power. {Priority One}

Indian Air Force

The cybersecurity policy 2018 of the Indian Air Force (IAF) to be shared and integrated with the Joint Policy of the Armed Forces. {Priority One}

To explore whether 'Vayusenix' (An Operating System by Air Force) can be upgraded suitably and adopted into the operating system of the armed forces. {Priority One}

The IAF needs to secure government sanction for the organisation, establishment and other logistic impediments on top priority. Headquarters Integrated Defence Staff must ensure expeditious resolution of logistics to prevent an adverse effect on operational capability. {Immediate}

The training establishment at Bengaluru should be upgraded for joint training. {Priority One}

Institute special measures and complete access control for platform security and inside threats. {Immediate}

Defence Information Assurance and Research Agency (DIARA)

Following are the indisputable and absolute strategic imperatives for creation and operationalisation of DCyA:

- Immediate government letter sanctioning formation of a Defence Cyber Agency, its approved organisation with incremental manpower, the command and control and delegation of powers to the Commander of DCyA. (Immediate)
- Appoint Commander of DCyA/Cyber Formation, post essential staff and issue raising orders. (Immediate)
- Form a steering committee, headed by CISC and include stakeholders by issuing appropriate government letter. This committee would report to the Raksha Mantri and be accountable for timely operationalisation of the DCyA. A slippage of eight weeks or more to be brought to the notice of the Prime Minister/Prime Minister's Office, National Security Adviser, Chiefs of Staff Committee and National Security Council Secretariat, clearly stating reasons and recommended solutions {Priority One}
- Nominate a think tank with requisite domain knowledge and experience as a consulting agency for compressing time frame and creation of 'knowledge' through analysis of technical

developments and utility in the Indian context. {Priority Two}

- The DCyA should have a young profile and flexible policies with regard to tenure, promotions and cadre management. Merit must be acknowledged and rewarded. Selection should involve tests for aptitude, security consciousness, out of the box and innovative thinking and a never say die spirit {Priority One to Three}
- The DCyA must have supporting facilities for human resource, training and certification, technology, R&D, intelligence, cryptology, coding, language, networks and sensors, safe products and systems, policies, processes and battle drills, integration, military diplomacy, international cooperation and interaction with cybersecurity components in civil, including joint exercises {Priority One to Three}
- In the first year, the DCyA should provide a minimum of Two integrated teams which must be operational within 18 months. Thereafter, in the second year, capacity must be built for Three integrated teams and for Five teams in the third year. The teams must be constituted based on the task on hand and have a very flexible construct {Priority One to Three}
- Operational parameters, particularly for command and control of these teams and the integral elements would get formulated as we go on

Human Resource, Training and Certification

- The government must declare 'cybersecurity' as a separate cadre immediately. There is a strategic necessity to develop an eco-system to generate human resource with required skills {Immediate}
- At the national level, all academic institutions must be directed to include basic cybersecurity training as part of their curricula {Priority One to Three}
- The armed forces should identify academic institutions for training in different skills up to advanced and doctorate levels. Selected institutions are to be given grants or easy finance for establishing training facilities and employing highly qualified faculty. Selected people to be sent abroad for specialised training {Priority One to Three}
- The NCC, NSS and Police Cadets must have cyber wings and become nurseries of skilled resource, both for civil and armed forces {Priority One to Three}
- An Institute of Cybersecurity Professionals be formed to draw skilled and experienced resource, both from within the country and abroad {Priority Two}
- All military stations be directed to form 'cyber orientation clubs' open to families of armed forces personnel, both to create awareness and for talent hunting {Priority Two}

The focus of capacity building by the armed forces would be on:

- Identifying and protecting vulnerabilities in military cyber space
- Create escalating levels of expertise for cybersecurity
- High level of multidisciplinary expertise for deterrent capability
- Developing advanced knowledge for the future
- The primary thrust of training must be on detection of threats, containment of damages and recovery from cyberattacks {Priority One to Three}
- Specialised training to selected persons would be imparted in cyber offensive operations, deception, and network penetration and protection {Priority One to Three}
- Train 'Cyber Leaders' in planning, conduct and management of cyber operations at the operational and strategic level, both in standalone mode and integrated with Kinetic and Information operations {Priority One to Three}
- As a policy directive, cyber proficiency in the armed forces be created and organised at four levels: {Priority One to Three}
 - Level One: Cyber Literate
 - Level Two: Cyber Operators
 - Level Three: Cyber Warriors
 - Level Four: Cyber Leaders
- Establish skilling institutes, both covert and overt, for training in special operations, counter-intelligence, code breaking, cyber weapons, conduct of cyber operations, re-skilling and up-scaling, providing adequate mobility and opportunities for career progression {Priority Two to Three}
- Establish world-class training infrastructure to include one cyber range per geography to conduct theatre aligned specialised courses, create network simulation centres, data centres and laboratories for information management, supply chain integrity, cyber deception and cyber forensics {Priority One to Three}
- Ensure adequate vacancies and finance for language training. At least efficiency in one foreign language be made essential part of officers training and incentives be given as per language proficiency {Priority One to Three}
- Create a pool of 'Master Instructors' for training and for them to be available for crisis management in case of a major cyber intervention {Priority One to Three}
- Establish an online training and certification facility along with resource for content generation {Priority One to Three}
- Conduct military hackathons, competitions and give away awards to incentivise the seen face of the cyber workforce both to attract fresh talent as well as to keep existing talent motivated. The unseen face will also be equally incentivised {Priority Two to Three}

- Creation of indigenous capabilities in language, big data, analytics, artificial intelligence, cryptology, networks survivability and availability, and nation-wide connectivity are strategic operation requirements and imperatives. We must establish an eco-system at the earliest and involve all stakeholders {Priority One to Three}

Recommended Approach for Technology Development

- Establish a 'National Mission for Information/Cybersecurity Technologies Development', to be headed by a technocrat and members drawn from stakeholders, including representatives from users, private industry, academia and the R&D establishment {Priority One}
- Carry out a detailed analysis of present and emerging technologies and related threats. Home into technologies that are needed with timelines for their development to support the doctrine. Some of these technologies, however, would have to be developed with higher priority to meet the immediate security requirements of the defence forces. For offensive operations, the making of cyber weapons and deception, we would need application-specific technologies {Priority One to Three}
- Create/award dedicated 'Projects' for the development of each technology, its transformation from engineering into production, integration and upgradation. These projects to

be awarded to a consortium of companies/institutions in a PPP model with 'womb-to-tomb' commitment {Priority One to Three}

- Timelines for implementation of each phase must be clearly specified with a provision for penalty in case of slippage and incentives for early completion within the budget and for innovations {Priority One to Three}
- The project director/lead company to have complete responsibility and accountability, be suitably empowered and to have assured access to finance {Priority One to Three}
- Attractive provisions and incentives for start-ups and involvement of medium and small scale enterprise {Priority One}
- Ensuring availability of human resource and training facilities
- Review/Revise National Electronic Policy – 2012 and give it strong impetus {Priority One to Three}
- Hire a foundry for semiconductors from a friendly country and concurrently commence deliberation for a foundry in India {Priority One to Three}

Contractual Clauses for System Protection and Availability

- Supply chain vulnerabilities will remain a major cause of concern for ICT networks and systems of the armed forces till such time as basic infrastructures for the manufacturing of chips and network products are not set up in India. Therefore, vendors must be bound by contractual obligations to

ensure due diligence from the issue of Request for Proposal (RFP) onwards for protection of networks and data to mitigate against vulnerabilities of cross-border supply chain. They must be made accountable for any systems failure on their watch {Priority One}

- Vendors must adhere to Indian law, including the Data Protection Law to be announced shortly {Priority One to Three}
- Contracts may include:
 - Cyber insurance and its operability as per the Indian legal system
 - Restrictions with regard to access, processing and sharing of data
 - A clause prohibiting remote access by vendors for maintenance and repairs of systems
 - Procedures and obligations for disaster recovery and business continuity as part of ensuring system resilience
 - Provision of an Escrow account
 - Overall security and adherence to the Indian Official Secrets Act
 - Training on secure codes, and
 - Maintenance of software codes as per the Software Licensing and Protection (SLP) contract

Emerging Threats and Negation Technologies

Today we are facing 5th generation cybersecurity threats wherein attacks are multi-everything – multidimensional, multi-stage, multi-vector and polymorphic. To properly

protect an enterprise's IT operations today requires a new, holistic approach to assessing and designing their security towards an integrated and unified security infrastructure that prevents attacks in real time.

The building of cyber-security into applications is critical in addressing such risks, as well as all the devices that are interconnected from the very beginning.

As attackers improve their capabilities, the armed forces must improve their ability to control access and protect their systems from attacks.

The armed forces must formally engage with security and risk leaders, evaluate the latest technologies to protect against advanced attacks, better enable digital operational transformation and embrace new computing styles such as cloud, mobile and DevOps {Priority One to Three}

India has to develop its own technologies, electronic manufacturing base, R&D infrastructure and highly skilled human resource. Being late has an advantage of 'leap ahead', but delay can have catastrophic consequences. There is a need to encourage industry, provide a level field, encourage start-ups and MSMEs and create a vibrant eco-system. {Priority One to Three}

- One will have to study and analyse adverse security effects, if any, of the involvement of foreign companies in building our infrastructure {Priority One to Three}
- Cybersecurity and cyber power are complex subjects. The armed forces would need some agency to translate their operational requirement into

identifying and exploiting the relevant technologies. It is for this reason that the task force has recommended an organisation like the Weapons and Electronics Systems Engineering Establishment (WESSE) of the Navy, staffed appropriately both with the Army and Air Force. Further, scientific advisers to the service chiefs will have to play a more active part {Priority One to Three}

Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence

Cyber power integrated with EW and Kinetic capabilities present exponential capabilities in creating deadly and desired effects. The armed forces must develop processes and drills for synergetic application in the digital battlefield to have force multiplication effect. {Priority One}

India needs to build all elements of cyber power to develop deterrence capabilities, both 'deterrence by defence and resilience' and 'deterrence by retaliation'. {Priority One}

Cyber power is offence dominant and in essence, a sum of intelligence, technology, information sharing, skilled human resource and total synergy. Our culture, actions and policies must reflect these {Priority One}

- Computer Network Operations (CNO) are increasingly finding acceptance as an attractive, low cost and low technology asymmetric option to undermine sovereignty, target individual leaders and engineer social discord. Accordingly, India must have the ability to protect her

assets from such cyberattacks and launch debilitating offensives, both to convey her resolve and credibility of deterrence {Priority One}

- Space-based assets play a crucial role in surveillance, intelligence, navigation and communications. Many nations are developing and testing anti-satellite weapons. It is a matter of time when conflicts will be from, to and in space. Integrated cyber and EW capability provides an alternative and potent option for anti-satellite operations. India must develop this capability at the earliest {Priority One to Three}
- The Internet of Things (IoT) is another fast developing capability for surveillance and cyberattacks in the cognitive, physical and electronic domains. Interference in IoT-based applications of major platforms like aircrafts and ships, present a very serious challenge to our systems and an extremely attractive opportunity for offensive tasks {Priority One to Three}
- Aircrafts, drones, helicopters and some classified space assets have highly integrated cyber and EW systems capable of both logical bombing and remote injunction of computer viruses. We will have to closely examine this capability and develop appropriate systems and processes for defensive and offensive tasks {Priority One to Three}
- There is a definite requirement for integrating the capabilities and resources of cyber and PsyOps, both in planning and execution.

Social media, in our context, is a very powerful dual-use weapon. While we need to quell false news and propaganda, we must integrate all necessary capabilities by way of language, technology, content and so on to effectively conduct 'media warfare' {Priority One to Three}

Cyber power can be applied by itself and in cyber-enabled operations in conjunction with kinetic weapons. Its biggest utility is as a 'Weapon of Information' in cognitive operations and perception management.

- Concepts would have to be developed for integrated application in accordance with the Indian Armed Forces doctrine. While training abroad is a must, the learnings would have to be transformed to Indian requirements. This calls for a very innovative, mentally agile and highly skilled human resource {Priority One to Three}
- Each Service must have a cyber range and a network simulation facility for regular training. Cyber operations, as part of IW, must form part of every war game, the deductions debated and the conclusions recorded, disseminated and incorporated suitably in battle drills {Priority One to Three}

International Engagement and Legal Framework

International Engagement

While defence and deterrence are effective in the short-term, cyber diplomacy holds more promise to contribute towards peace and stability in the long run. India needs to take

a leadership position in various international initiatives taken at the level of United Nations, International Telecommunication Union (ITU), regional bodies and autonomous organisations like the Internet Corporation for Assignments of Names and Numbers (ICANN), Internet Engineering Task Force (IETF), etc.

Diplomatic influence needs to be exerted to secure a leading position in the above organisations, both for policy formulation and for dealing with large-scale cyber interventions.

The armed forces need to be actively associated with:

- Cyber diplomacy, because as opposed to overall cyber defence, diplomacy offers higher potential for conflict de-escalation, and thus, for developing norms of state behaviour, that needs to be implemented by the armed forces for peace in cyberspace {Priority One to Three}
- Formulation and orchestration of international norms that would limit disruptive activity by states against other states and deter non-state actors {Priority One to Three}
- The task force recommends the following for furtherance of stated objectives of the Indian Armed Forces Cyber Doctrine: {Priority One to Three}
 - India needs to play an active and constructive role in international cyber diplomacy to pursue national security interests
 - Cyber diplomacy should be an indispensable component of military dialogue and diplomacy

- The central role of the UN in Internet governance and the primacy of the state in cyber conflicts need emphasis
- International consensus on norms of state behaviour needs to be pursued on bilateral and multilateral platforms despite the failure of UNGGE 2017

Legal Aspects

The environment must be made aware of the provisions of Article 51A, which empowers the government to enlist qualified manpower for quick boosting capacity of cyber warriors in case of a cyber war. {Priority One to Three}

Define Indian cyberspace jurisdiction as follows: {Priority One}

The Indian cyber-physical territory includes, but is not limited to the embassies, the high commissions, the consulates, satellites and systems owned by the Indian Armed Forces such as aircraft, ships, submarines, tanks and or any other ground vehicles. It is recommended that India may exercise her cyberspace jurisdiction:

- Over an entity or a person who is engaged in cyber activity on her territory
- Over the objects related information technology located on her territory
- Over data and content process over her territory
- Extraterritorial
 - Over data or content which is being stored processed or transmitted belonging to the entity or cyber

infrastructure which is within Indian territory or legal jurisdiction

- Over the entity, person, cyber infrastructure, data and content which is the source of or abettor of a devastating cyberattack on any object or person or cyber infrastructure based within the jurisdictional Indian cyber territory
- Extraterritorial, in accordance with the international laws, treaties and agreements

Establish nation-wide cyberwar fighting processes and procedures as Cyberwar Standard Operating Procedures (CyWar SOP). These will form the basis on which cyber war games, drills and exercises would be conducted and measured. {Priority One to Three}

Amend Section 69 of the Information Technology Act to provide for any situation related to cyber war or defence against cyber war and empower the concerned defence officer to intercept, monitor and decrypt any information on computer resources. {Priority One}

Promulgate a Cybersecurity Act that would cover not only various cyber-related crimes, offences, forensics and policing, but also, have enabling provisions for cyber war and defences against cyber war. {Priority Two}

- India with its significant manpower and technical know-how should proactively support weaker nations to establish their cyber defences. It will:
 - Help project India as a reckonable cyber power

- Prevent these nations from becoming a source of cyberattack on India
- Prompt these nations to become strategic partners in case India faces a cyber offensive

Cyber forensics plays a critical role in cyber war to prove any stand in any court of law, Indian or International. Therefore, it must be an intrinsic part of cyber power in the armed forces. {Priority One to Three}

Cyber forensics is also necessary for cyber battle damage assessment and to recalibrate for the next attack. Cyber forensic experts must be embedded in cyber forces to meet legal and international obligations. {Priority One to Three}

The Rules of Cyber Engagement (RoCyE) should be defined for the uniformed forces and other cyber forces. To implement RoCyE, there should be a state of alertness/readiness which must be defined. {Priority One to Three}

- Following 'State of Readiness', flags are recommended {Priority Two}
 - Blue – Normal state
 - Green – Enhanced cyber intelligence/surveillance by Nation State/reckonable Non-state actor
 - Yellow – Cyberwar likely
 - Orange – Cyberwar imminent
 - Red – Cyberwar in progress

Supporting National Institutions, Policies and Infrastructure

The task force recommends establishment of the following institutions. Details given in the main paper.

- National Cybersecurity Commission (NCSC) {Immediate}
- Cyber Policy Research Centre {Priority One}
- Integrated Cyber Threat Intelligence Centre {Priority One}
- Indian Cybersecurity Operational Centre {Priority One}
- National Cyber Test Facility {Priority One}
- Information Management and Assurance Agency {Priority One}
- National Centre for Cybersecurity Resilience {Priority One}
- Cyber Command {Priority One}

Policies and Infrastructure

- Prepare and issue a National Integrated Cyber Doctrine {Priority One}
- Establish a National Academy of Information Security {Priority One}
- Revise National Electronic Policy-2012 and carry out aggressive implementation {Priority One}
- Revise National Cybersecurity Policy-2013 {Priority One}
- Create a formal military-industry interface to secure products and software {Priority One}
- Depute a think tank to lead and form an Institute of Cybersecurity Professionals {Priority Two}
- Develop standard operating procedures for executing a cyber war {Priority Two}

- Undertake a nation-wide cyber war exercise at least every alternate year {Priority Three}
- Initiate process for formulation and approval of a Cybersecurity Act {Priority Two}

Budgetary Assurance

The development of cyber power in the armed forces has been sluggish and disjointed. One of the reasons is the paucity of funds. Consequently, today the country is vulnerable with regard to information security as compared with likely adversaries. We have to make up for lost time. The availability of funds, empowerment, delegation of financial powers, carry over of unspent money to the next financial year, committee-based decision making and pre-audit are some of the essential factors. The main issue is capacity building in cyber power must have the total support of the government along with complete assurance of fund availability.

As a ballpark figure, budgetary allocation of Rs 6,000 crores over the next three years, exclusively for building cyber power may be made. What is not negotiable is the assurance of availability of finance from the highest political authority. {Priority One}

Road Map and Action Plan

The road map is illustrated in the summary of recommendations, but any plan is only as good as its implementation. With regard to developing cyber power for our defence forces, two cardinal principles of 'System Approach' and 'Concurrency' must be adopted. An action plan must be introduced by different entities through astute project management,

delegation of powers and monitoring at the highest level. It is surprising that in spite of the Prime Minister's clear pronouncement during the Formation Commanders conference in 2014, cyber power development in the defence forces has been minimal. This calls for introspection and an aggressive mission-oriented approach to remove bottlenecks.

The task force has recommended capacity building in support of the stated doctrine within 36 months, which encompasses sanction and transformation to a full-fledged Cyber Command and recognition of India as an emerging cyber power.

The starting points would be the issue of necessary government sanctioning letters, an appropriate organisation for project management, forming a steering committee and fund allocation.

The nominated organisation must have a director for each of the seven pillars. This would be a tri-service organisation under HQ, IDS and would deliver a quarterly progress report to the Chiefs of Staff Committee.

Finally, the task force would like to place on record their thanks to Dr. Arvind Gupta, Director, VIF and Lt. Gen. R.K. Sawhney, PVSM, AVSM, Centre Head and Senior Fellow, VIF, and the VIF staff for their support. It is emphasised once again that urgent capacity building of cyber power in our armed forces is a strategic necessity. We hope this report will help the powers that be in quick decision making.

PART II

Cyber power is an ideal tool for conducting asymmetric warfare and to convey cyber deterrence capability. While underdeveloped and developing nations are busy preparing for offensive cyber operations, the developed nations, due to their increased vulnerability, are concentrating on defensive cyber operations with active defence as part of their doctrine. The scenario is, however, changing with developed nations going for credible offensive capabilities, development of cyber weapons and propagating the idea of 'Cyber Deterrence'.

Section One

Policy and Strategy for Cyber Deterrence through Development of Cyber Power in Indian Armed Forces.

Environment Scan

Cyberspace has become a full-blown war zone as governments across the globe clash for digital supremacy in this new and mostly invisible theatre of operations. Electronic technologies, Electro Magnetic Spectrum and an estimated seven billion people make cyberspace unique. An increasingly wide range of social, political, economic and military activities depend on cyberspace, making it both a much sought after capability and vulnerability. Cyberspace has truly become a tool for 'virtual expansionism', the only limit being the innovation of people.

As the Industrial Age gave way to the Information Age, the quantity and speed of information transfer has grown, as has its penetration into society. This evolution has resulted in physical force being supplemented by additional forces – content and code (information and computer software) – that can influence all three elements of the 'Clausewitz's Trinity' nearly instantaneously and simultaneously.

The accelerated intertwining of cyberspace and human activity in recent decades has given rise to both a new domain and new form of warfare, which is man-made, is in constant transformation and demands understanding by both civilian and military leaders. It is for the first time that human security is so threatened and that puts extra pressure on governance and on organisations chartered with their security.

Once limited to opportunistic criminals, cyber-interventions are becoming preferred weapons for governments seeking to defend national sovereignty and to project national power. From leaking debit card details to influencing the US presidential election, cyberattacks have become a significant part of our political and social discourse.

The exponential rise of 'cyber power' in a short span of four decades is both amazing and mindboggling. From cyber-crimes to cyber espionage to cyber terrorism to social engineering to cyber war and now cognitive dimension for the management of human behaviour, there have been substantial enhancements in each of these capabilities by way of people, processes, complexity and technology.

Technology and organisational innovations over the last few decades have not only fully transformed the nature and character of the battlefield but created the potential of 'non-obvious warfare'. Types of warfare that could be conducted in a non-obvious manner include cyber warfare, space warfare, electronic warfare, drone warfare, sabotage, special operations, assassinations and mining, proxy attacks, WMD and intelligence support to combat operations. Cyber power can influence all these types of warfare and other war-fighting domains.

The 21st century battlefield is largely digitised with largescale deployment of

Information and Communication Technologies (ICTs) in every facet, from C4ISTAR, information management, weapon systems in all domains that is ground, air, sea, outer space and cyberspace down to the individual soldier.

A digitised battlefield has made national borders irrelevant, challenging the very concept of national sovereignty and is a place where operations are conducted at the speed of light. Typically, a digitised battlefield will be shaped continually by the national doctrine and would remain a work in progress due to the rapid march of technology and its consequent impact on the conduct of war. We experience that human and international conflicts are entering a new phase in their long histories. In this shadowy battlefield, victories are fought for with bits instead of bullets, malware instead of militias and botnets instead of bombs.

To understand the application of cyber power, it is essential that one comprehend the Information Environment (IE), for what moves through cyberspace is information in the form of code (software) that gets displayed as content on a graphic user interface (GUI). The IE could be described as, 'The aggregate of individuals, organisations and systems that collect, process, disseminate or act on information across the physical, informational and cognitive dimensions'. These IE dimensions are inextricably linked, resulting in cyberspace operations increasingly being used to manoeuvre in support of both civilian and military objectives.

Militaries and civilians alike now use cyberspace operations to achieve objectives concerning communications, targeting, navigation (global positioning systems– GPS), logistics, training, education, shopping,

banking, entertainment and more. Cyberspace has driven changes in the economy and domestic politics in many nations, with social media helping to change political power. Radical ideology and political agendas are being spread globally in near real time.

Cyber power is an ideal tool for conducting asymmetric warfare and projecting cyber deterrence capabilities. While underdeveloped and developing nations are busy preparing for offensive cyber operations, developed nations, due to their increased vulnerability, are concentrating on defensive cyber operations. The scenario is, however, changing with developed nations going for credible offensive capabilities, development of cyber weapons and propagating the idea of 'Cyber Deterrence'.

Several nations have formed military cyber commands and many more are considering similar changes to government and military command organisations. Al Qaeda and its associated movements (AQAM), Anonymous, and the Russian Business Network are examples of non-state actors that use the domain for nefarious acts at will. The Islamic State of Iraq and the Levant (ISIL) is actively pursuing military-style cyber capabilities.

Global ICT corporations have equal access and vested interests in manoeuvring in cyberspace to achieve corporate economic objectives. These corporations also provide much of the key connectivity necessary for governments and militaries to manoeuvre. They will have to take on the responsibility of providing uninterrupted services with resilience.

Cyberspace is thus an 'integrated civilian and military domain'. Military forces must

collaborate with civilian-owned, managed and operated cyberspace elements to achieve the desired effects. This interaction blurs the lines when military actions begin and end compared to those of civilian organisations.

The Indian Scene

India is very vulnerable to cyber interventions due to certain strategic deficiencies, absence of a clear-cut policy directive and cyber warfare doctrine; ongoing transformation to digital economy and its fast pace; inadequate appreciation of the threats, both internal and external; a cavalier attitude towards security and law; lack of synergy between government organisations and private industry, extreme shortage of skilled human resources and inadequate implementation of policies. Resultantly, India has only certain islands of cyber power; grossly insufficient as compared to the threats and its national security needs.

India was among the handfuls of nations to promulgate the Information Technology Act in the year 2000 to deal with cyber interventions. The same was revised in 2008. Similarly, the National Policy on Electronics was issued in 2012 and the National Cybersecurity Policy (NCSP) in 2013. Yet, till a few years ago, well-co-ordinated and focused efforts towards cybersecurity were missing, except for the establishment of the Computer Emergency Response Team – India (CERT-IN) and similar organisations at the state level and the defence forces.

India has since adopted an integrated approach and conceptualised a cybersecurity architecture with emphasis on protection of critical information infrastructure,

capacity building in terms of indigenous ICT technologies, R&D, human resource development and public-private partnership on cybersecurity issues. The salient aspects of this architecture include:

- Operationalisation of a National Critical Information Infrastructure Projection Centre (NCIIPC)
- Establishment of the National Cyber Coordination Centre (NCCC) by MeitY for threat management and information sharing in real time
- Establishment of Cybersecurity Assurance and Certification Bodies for testing, evaluation and cybersecurity audit
- Creation of an R&D fund for setting priorities for research, indigenisation and human resource development
- Public-Private Partnership on cybersecurity
- Capacity building and creation of 500,000 Cybersecurity professionals

The National Security Council Secretariat (NSCS) coordinates and oversees cybersecurity issues, including cyber diplomacy. The National Cyber Security Coordinator at the NCSC has been entrusted with the responsibility of coordinating and synergising cybersecurity efforts

According to the National Cyber Security Coordinator, India, by 2020, will face increasingly sophisticated 'destructive' cyber threats as compared to the 'disruptive' attacks in Indian cyberspace that are currently adding up to 200 million malware-related and 190,000 'unique' intrusions in any given week. Coupled with this is the likely threat from our adversary

which is recognised as an emerging cyber superpower with full spectrum capabilities.

Surprisingly, the NCSP-2013 does not talk about the creation and application of cyber power, the role, organisation, equipping and training of the Indian armed forces to execute cyber-enabled operations and cyberwar, leaving a glaring gap in policy with regard to national security. In the prevailing environment of potent threats, direct and indirect in the cyber domain, and the likely degradation of our fighting potential, social engineering directed towards causing a perceived failure of governance and fake news, this is a very serious strategic deficiency which is required to be overcome without delay. India does not have time as the strategic window is closing very fast. We, very urgently, need to enunciate our national cyber power policy and doctrine, build 'Cyber Power as a System' commensurate with India's standing and security needs, and integrate it with other warfighting domains to enhance our national security across the full spectrum of threats.

This requires strong political will, total synergy between government and private sector, a dedicated and empowered organisation, assured finance, well-trained and highly skilled human resource with attractive emoluments and a flexible environment, training infrastructure, acceptance of cybersecurity as a government cadre, focused participation of private industry, electronic manufacturing base and components, particularly for 'secure' products; standards; international cooperation including joint exercises and sharing of incident reports; legal mechanism; R&D and testing laboratories; centres of excellence for cyber weapons; kill switches and analysis; language, coding

and crypto experts; specialists in information management and analysis; intelligence resource for interacting with the underworld/deep/dark web and more; backed by forceful and determined implementation in a mission mode due to the extreme shortage of time. These activities will have to be implemented concurrently along with spreading awareness amongst the masses about threats to their security, their responsibilities as citizens, promoting application of good practices and cyber hygiene.

In pursuance of above, the task force set the following aim:

'To prepare a roadmap and associated action plan for capability building of the Indian armed forces for cyber deterrence across the full spectrum, commensurate with India's standing and her security needs, and to integrate the same with the national cybersecurity eco-system.'

Approach to Capacity Building

Before we suggest approaches to capacity building, let us define 'cyber power' as perceived by us. Cyber power can be defined as:

- The ability to use cyberspace to create advantages and influence events in all operational environments and across instruments of power
- Cyber power is society's organised capability to leverage digital technology for surveillance, exploitation, subversion and coercion in international conflict
- Military cyber power can be defined as 'application of operational concepts,

strategies and functions that employ the tools of cyberspace to accomplish military objectives and missions.'

Seven Essential Factors Constituting Cyber Power

1. Internet and information technology (IT) capabilities
2. IT industry capabilities
3. Internet market capabilities: The size and scale of domestic Internet infrastructure is a major push factor
4. The influence of Internet culture: The reach and penetration of Internet triggering behavioural changes in people
5. Internet diplomacy/foreign policy capabilities: This is a nation state's bargaining power
6. Cyber military strength is the ability to defend critical national and military IT infrastructure from attacks, deterrent capability, the ability to conduct offensive operations in cyberspace and prevent espionage in own networks
7. National interest for taking part in cyberspace strategy: To be a cyber power, it is not sufficient for a nation-state to merely possess part or all capabilities. It depends upon the motive or willingness to use possessed power. The nation-state's cyber strategy must enunciate theoretical guidance, behavioural norms, criteria for action and a strategic plan.

An analysis of the above factors indicates that as far as penetration, infrastructure and culture of the Internet are concerned, India

is well placed, being the second largest user of the Internet globally. India needs to exert much more in international fora to ensure favourable terms with regard to Internet governance, positioning of hardware and legal framework.

India woefully lacks in cyber military strength when viewed from the perspective of threats and capabilities of exploiting this very potent and ubiquitous domain of warfare. The task force would present an action plan and road map to overcome this strategic deficiency and acquire cyber deterrence capabilities in consonance with India's standing amongst the comity of nations and the threats. Achieving this would be contingent on having the political will to develop capabilities and use them to ensure our national security and sovereignty.

For the sake of clarity and uniformity, the task force will lay down essential indicators of cyber power and then suggest a methodology for harnessing the same. These are:

- Infrastructure, including networks size and broadband penetration
- A clear international strategy that lays out priorities and defends a nation's right to have a voice on cyber issues
- Independent technological capabilities, especially in operating systems and central processing units
- The ability to defend networks, be it for national security, economic security, user privacy, social stability/harmony
- Competitiveness in development of software applications and e-commerce

- Recognition as a credible cyber power capable of influencing decisions

The Prime Minister, while addressing the Combined Commanders Conference in 2014, clearly stated the absolute necessity of transforming the Indian Armed Forces into a digital army in pursuance of the government's declaration of 'Digital India' as one of its major objectives. This transformation has been rather sluggish.

The government, very recently, has accorded approval for the raising of a Defence Cyber Agency (DCyA). This, at best, is a half-hearted attempt keeping in mind the perceived threats and India's geopolitical role.

The Task Force recommends that the formation of DCyA be taken as an intermediate step towards the formation of a full-fledged Cyber Formation/Cyber Command in the next three years while concurrently developing capabilities for full spectrum Information Warfare with Cyber Power as one of its major constituents.

The task force has, accordingly, decided that it would follow two clear and concurrent approaches i.e., to concentrate on capability building of the armed forces and integration with the national cybersecurity architecture at a macro level.

Cyber power of our armed forces must be based on the Seven Pillars below:

Seven Pillars for Capacity Building

1. Policy and strategy for development and employment of cyber power
2. Indian Armed Forces Doctrine for application of cyber power and information operations
3. Organisation for cyber deterrence, synergy, staffing and adaptation of cyber force
4. Human resource, training and certification
5. Technology, R&D, standards and integrity of data
6. Integration and development of concepts for effective cyber deterrence
7. International engagement and legal framework

Note: FORMATION vis-à-vis Agency

A 'Formation' is an organisation entity in the Indian Army like a Brigade, Division, Corps and Command. There is no organisation like an 'Agency'. Raising of Defence Cyber Agency is perhaps the lowest in the rung, not well understood, has limited resources and would not be in a position to convey 'Deterrence' as stated in the recommended Cyber Doctrine for Indian Armed Forces.

Accordingly, the Task Force felt that while Defence Cyber Agency is a long awaited and welcome measure; it must provide the base for an Indian Cyber Command which must be created within the next three years to effectively respond to the likely and emerging threats.

Since, one is not certain of the government's likely decision, the report has expression like 'Formation/DCyA'. Formation conveys the organisation level of cyber power, (cyber brigade/division/corps/command) and is a familiar entity, hence well understood. Recommendations made in the report are equally valid to both, the Formation and Defence Cyber Agency.

Further, the terms convey the long-term applicability and validity of the report as the DCyA transforms to a Cyber Command.

“One should never submit spinelessly, nor sacrifice oneself in foolhardy valour. It is better to adopt such policies as would enable one to survive and live to fight another day.”

– 7.15.13-20,12.1.1-9 Arthshatra by Chanakya

Section Two

Policy and Strategy for Developing Cyber Capability of the Indian Armed Forces

Cyber-enabled armed forces and creation of cyber command are aimed at addressing a critical void in developing India's fifth-generation warfare capability in a digitised battlefield.

Introduction

Within the ambit of Information Warfare, cyberspace has emerged as a distinct new man-made domain. Specific policies, strategies, organisations and techniques are required for operating in this domain, and are quite akin to those required for operations on land, air, outer space and maritime domains.

To evolve a policy for operating in this domain, a comprehensive review of the threats that can emanate in cyberspace and potential targets need to be identified and a determined response mechanism be put in place to counter it. Various stakeholders need to be identified and national level organisations evolved for synergising activities across different departments/organisations. Thereafter, cyber resilience and deterrence strategies need to be evolved to meet national security requirements in consonance with appropriate domestic and international laws. A strategy also needs to be worked out to optimise and create hardware and software, plan future technology development, impart training, certification and create a pool of skilled manpower. Being an activity that transcends national borders, an international cyber cooperation strategy is required.

Aim

This chapter aims to evolve a cyber resilience strategy and a deterrence-enabled

armed force, capable of creating a secure cyberspace environment and to be a force multiplier for conventional operations in other domains.

Threat Scenario

India has about 500 million Internet users (2018 statistics) and this is likely to increase to 635.8 million by 2021. Internet penetration is a measure of the extent of reliance on net-enabled services by common citizens, business, critical information infrastructure, military and government. In this domain, it is hard to draw clear boundaries between military and non-military users since cyber operations go beyond a single domain. Also, cyberspace challenges emanate both from state-affiliated and non-state actors and can impact all elements of national power (diplomatic, informational, economic and military) concurrently through manipulation of data and gateways.

Cyber threats manifest in many forms and may result in serious disruption of government, public and private sector resources and services – impacting lives, the economy and national security.

India has been amongst the worst-affected countries from global cyberattacks in the recent past. The 2017 WannaCry ransomware attack affected about 48,000 computers. The Stuxnet malware attack in

2010 affected about 10,000 computers in India, some of which belonged to critical infrastructure facilities, including power grids and offshore oil rigs of the Oil and Natural Gas Corporation. The Nuclear Power Corporation of India, by its own admission, blocks at least 10 targeted cyberattacks a day. Closer to the conventional security domain, Indian security forces regularly confront cyber radicalism from extremist groups who use the web to spread propaganda, incite violence and plan and carry out catastrophic attacks.

While India promulgated a National Cybersecurity Policy in 2013 with an integrated vision and strategies for implementation, in practice, the application of this policy remains dispersed (fragmented) across different sectors. The overall approach has remained that of strengthening cyber defence and enhancing survivability. Cyber space has not been viewed as a domain for the conduct of warfare.

Characteristics of Cyber Warfare

Some peculiar characteristics of this domain are:

- **Asymmetric nature of warfare.** Cyberattacks can be launched by a much weaker adversary (militarily, technologically and economically), or even by non-state actors at negligible cost. Also, the positioning of 'cyber attacks' in the escalatory ladder of conflicts still remains ambiguous. These could well be situated from the lowest end of the spectrum to upper-end strategic conflict levels
 - **Anonymity.** It is difficult and time-consuming to identify perpetrators of
- the attack. Even on being detected, a reasonable scope of deniability exists
- **Neutral (or innocent) third country involvement.** Many cyberattacks may originate from co-opted servers in neutral countries, at times without involvement or knowledge of those countries. The culpability of such countries and the legitimacy of actions against them still remains ambiguous
- **Ambiguity in defining 'Attacks'.** An acceptable definition of a 'cyberattack' which would justify retaliatory punitive action, including physical (kinetic) retaliation, does not exist yet
- **Grey Zone of 'Cyber Espionage'.** Cyber intrusions are extensively used for 'cyber espionage', which may be related directly to gathering military intelligence or be aimed at industrial espionage, or theft of commercial information. Despite such cyberattacks being directed against the nation's military/defence capability, the legitimacy of counter-attacks in the cyber or physical domain remains suspect
- **Absence of objectives for retaliation.** Originators of cyberattack, even if identified, may have no assets or organisational interests to be retaliated against. The retribution may ultimately need to be in the elementary kinetic domain
- **Cross Domain Linkage.** Cyberattacks against targets in a particular sphere may result in cross-sectoral disruption. For example, intrusion into networks controlling critical civilian infrastructure, power grids,

transportation networks and financial systems can have national security/military implications. No distinction can generally be drawn between civil and military targets, except those attacks which are directed purely against military weapon systems and networks

Military Targets for Cyber Warfare

In a generic sense, information, information systems and networks constitute cyber warfare targets. In the military domain, these targets can be grouped broadly into the following categories:

- Command, control, communication, computer, intelligence, surveillance, reconnaissance and logistics networks (C4 ISR L) and systems
- Critical information storage systems which may contain classified operational plans, intelligence data, critical technology and weapon control data
- Decision support and fire control systems
- Navigation and guidance systems of complex platforms like aircraft, ships, missiles, drones and precision-guided munitions
- Assets in outer space and their supporting infrastructure on earth
- Exploiting the cognitive domain aimed at change in behaviour and undermine the morale of combatants through well-orchestrated disinformation campaigns and perception management activities

Role of Cyber Formation/Defence Cyber Agency

- Defending own computer networks, platforms and weapon systems
- Defence against foreign origin or foreign-sponsored cyberattacks, especially if they can cause loss of life, property, or significant foreign policy and economic consequences
- Synergising cyber intelligence with signals intelligence, Electronic Intelligence (ELINT), Human Intelligence (HUMINT) and operational security for a comprehensive threat analysis in the information warfare domain
- Provide offensive cyber options to be implemented on approval, as force multipliers for other operations. This would include covert operations
- Plan and execute cyber deception
- Recruit, train, retain and periodically refresh human resource, equip them and be responsible for cadre management
- Be a part of military diplomacy and exchange of information with friendly nations, joint training and integrated approach for Internet governance, legal framework and favourable policies
- Effective liaison with civilian counterparts for policy making, processes, exchange of information and ensuring interoperability of systems

- Establish suitable organisation for information assurance and management
- Create system and infrastructure for training, laying down of policies and processes
- Establish technology research facilities by the Services and jointly with the private sector
- Ensure requisite budgetary support and effective liaison with other agencies, academia and R&D establishments

Policy for Creating Cyber Warfare Enabled Armed Forces

IT systems are used in all spheres of national activity, including in the armed forces. All sectors remain responsible for creating a robust and secure system within the guidelines contained in the National Cybersecurity Policy-2013 and regulations that may get included in future and the Data Protection Law.

For the present, the overall organisational structure for managing cybersecurity at the national level would remain under the National Security Adviser and the National Cybersecurity Coordinator. The Indian Computer Emergency Response Team (CERT-IN) and the National Critical Information Infrastructure Protection Centre (NCIIIPC) would perform the primary functions of managing protection and resilience of the nation's critical information infrastructure. These agencies, in close coordination with the National Technical Research Organisation (NTRO), would also be responsible for obtaining strategic information relating to ICT infrastructure threats and evolving a crisis management mechanism

through effective predictive, preventive and protective, response and recovery actions. These functionalities have been announced in the NCSP-2013. The Cyber Formation/DCyA must be integrated with these organisations for offensive tasks and deception. Information must be shared with complete transparency on a real-time basis to ensure synergy and delivery of requisite effects.

Cyber warfare enabled armed forces and Cyber Formation would provide a dedicated, trained and equipped military organisation to execute all operational aspects in this domain. Cyber Formation/DCyA would work in concert with the cyber organisations of each individual sector/department, including the three Services.

This organisation would be responsible for the conduct of cyber support operations, including intelligence collection, collation, analysis and dissemination, cyber deterrence, formulation of prioritised cyber target lists of potential adversaries; plan and execute retaliatory offensive operations; conduct testing and certification of hardware and software; assist in development of indigenous technologies and weapons including cryptology and cryptoanalysis related tools; conduct training and cyber exercises; and management of international cyber cooperation.

Cyber Formation/DCyA would also need to have a robust legal component to ensure that operations are conducted in accordance with the rules of engagement that comply with international and domestic laws and that enough legal justification exists for transcending to physical conflict (Kinetic offensive action), should it become necessary.

Cyber Formation would be responsible for planning and conduct of Cyber Offensive Operations, deception and cyber exploitation particularly related to likely targets, vulnerability assessment, probing missions, penetration testing and exploitation of adversary's networks. It will be responsible for complete information management and information assurance.

Strategy

The strategy for creating and operationalising cyber-enabled armed forces (DCyA/Cyber Formation) should be based on the following factors:

Creation of an appropriately 'situated' and 'constituted' operational formation for all aspects of 'application of cyber power' including cyber warfare.

The organisation will address issues in the military and civil domains, including critical infrastructure within the overall national cybersecurity organisation as evolved through the National Cybersecurity Policy. It must be synergised with all other ministries, significant R&D organisations and strategic industry. The onus of overall coordination and specific tasking along with a delegation of appropriate operational and legal authority would, however, rest with the National Cybersecurity Coordinator for the present.

Delineation of Responsibilities. The primary responsibility of cyber defence, including that of the existing governance networks (.gov/.nic) would rest with respective ministries, departments, organisations and industry. Similarly, the Army, Navy and Air Force would be responsible for their basic cybersecurity to include cyber resilience and defence in depth. The cyber command would

be responsible for specific military aspects, as given above. Notably, it would also be the only organisation within the country to be authorised, equipped and trained to conduct offensive cyber operations including those related to strategic intelligence and deception.

Enforcing Implementation of Cybersecurity Policy. The Cybersecurity Organisation will be responsible for formulating and promulgating information security policies, while the Cyber Formation would be responsible for enforcing compliance. It would also be responsible for testing and validating all software and hardware to be used, particularly in critical areas. It should also be responsible for setting up facility for examining and certifying all hardware procured/manufactured.

Evolving Rules of Engagement. Time-critical detection, identification and retaliation necessitates formulation of legally tenable and robust rules of engagement for responding to cyberattacks. Launching of counter-offensives would be a command decision based on necessity, appropriateness and proportionality of response. Commanders would determine the appropriate level in war or peace. Responsibility and authority would be vested in the Cyber Command.

Contingency Plans for 'Degraded Operations'. Despite robust cyber defensive measures, penetration of cyber networks cannot be ruled out totally. The Cyber Command would need to evolve and rehearse continued execution of operations in different spheres, albeit with degraded capability. Manual or standby infrastructure, operating procedures and manning staff would need to be planned for as part of operational contingency.

Training. The National Cybersecurity Policy has envisaged training of approximately 500,000 personnel in a time span of about five years (commencing 2013). The Cyber Command would need to assume responsibility for imparting specialised training aimed at creating superior military capabilities in cyberspace. Some of this training may have to be conducted through public-private participation by incorporating technology majors. The Cyber Formation would also be responsible for establishing simulator training, and for setting up and managing the National Cyber Range.

Outsourcing and TAisation of Cyber Organisations. Due to the peculiar nature of cyber operations, the Cyber Command would need to be structured and empowered to selectively outsource operations. Alternatively, it may also resort to employing select embodied personnel (akin to Territorial Army [TA] battalions). This would provide an opportunity for inducting personnel with proficiency in contemporary cyber technology and the benefit of deniability (anonymity).

Evolving Cyber Technology Perspective and Capability Road Map. Cyber Formation with cross-domain and international linkages, including with the IT industry and R&D organisations, would be best suited to carry out perspective planning for the IT and cyber domain in the overall context of information warfare. It could also be used as a single point contact for equipment acquisitions, which are time-consuming and result in acquiring of equipment with redundant/outdated technologies. Also, in case of cyber warfare equipment, the acquisitions be made as applicable for strategic systems, rather

than adhering to the Defence Procurement Procedure (DPP).

Conclusion

The cyber domain has inseparable linkages between the civil and military spheres. Cyberattacks directed against government, critical infrastructures, economy, military, industry and so on, have cross-domain implications. The peculiar nature of attacks, with inbuilt anonymity, deniability and legal implications of defining the nature of attacks make cyber defence and retaliation a complex phenomenon. While the country has developed cybersecurity capability, this sphere has not yet been addressed as a domain of specialised asymmetric warfare.

Cyber-enabled armed forces and the creation of a Cyber Command is an endeavour to address this critical void in developing India's fifth-generation warfare capability in a digitised battlefield.

‘Doctrine is indispensable to an army. Doctrine provides a military organisation with a common philosophy, a common language, a common purpose, and a unity of effort’.

– General George H. Decker, 1960

Section Three

Indian Armed Forces Doctrine for Application of Cyber Power and Information Operations

India needs an 'Integrated National Cyber Doctrine' developed jointly by the civil authorities and the Armed Forces with 'Cybersecurity' aspects dealt with by the civil authorities and 'Cyber Power' by the Defence Forces.

This doctrine may be read in conjunction with the following documents:

- Joint Doctrine Indian Armed Forces 2017
- Joint Training Doctrine Indian Armed Forces 2017
- National Cybersecurity Policy (NCSP) 2013
- National Policy on Electronics (NEP) 2012
- Information Warfare Joint Doctrine Indian Armed Forces
- National Policy of Digital Communications

Though not promulgated in the public domain, one would like to believe that two seminal documents – the National Security Policy and the National Security Strategy exist in some form. All three services have their respective doctrines and the latest is the Joint Doctrine of the Indian Armed Forces-2017 and the Joint Training Doctrine-2017.

The Joint Doctrine states that conflict will be determined or prevented through a process of credible deterrence, coercive diplomacy, and conclusively by punitive destruction, disruption and constraint in a nuclear environment across the spectrum of conflict.

Another important pronouncement under the 'National Military Objectives' is:

'Enable required degree of self-sufficiency in defence equipment and technology through indigenisation to achieve the desired degree of technological independence by 2035.'

This probably presents the biggest challenge, given the present state of the domestic defence-industrial complex.

The doctrine is a bold announcement. It talks about the TRIAD of Cyber, Space and Special Forces. The government has approved very recently the raising of a Defence Cyber Agency, a Defence Space Agency and a Special Forces Division. The real challenge now is how quickly we can operationalise these organisations and integrate them with the comprehensive national power. It must be appreciated that in the digital battlefield of today cyber power would be central to any capability for 'credible deterrence'.

India needs an 'Integrated National Cyber Doctrine' developed jointly by the civil authority and the armed forces with cyber security aspects dealt by the civil authorities and cyber power' by the defence forces.

In the absence of a National Cyber Doctrine and keeping in mind the threat landscape, both present and emerging, the task force recommended the following national cybersecurity architecture and kinetic capabilities:

- The employment of cyber power is subject to long-standing political,

economic, and military considerations – one of which is the need to minimise unintended and costly conflict among the parties involved

- States have become more skilled in employing these instruments over the past decade and have developed increasingly complex means with which to exploit vulnerabilities
- Cyber power is fast graduating from a disruptive to destructive component with exponentially increased potency when integrated with EW and kinetic power. Coupled with its ubiquitous nature, it is capable of altering the military balance
- Non-state actors, 'lone wolf' and 'insider threats' along with the anonymity of the attacker add another very challenging dimension to the threat landscape, necessitating international cooperation and complete synergy of own capabilities
- Many states, in their doctrines, have declared their right to respond with conventional military means to cyber threats and the operational requirement of cyber deterrence to reduce chances of conflict and to promote restraint
- Cyber espionage has become a major source of intelligence, discovering of vulnerabilities, proving of cyber weapons by probing attacks, and providing content for disinformation and perception management. Its importance can be gauged from the fact that nations are launching cyber espionage campaigns

- Cyberattacks are launched at the speed of light. Hence, cyber defence has to be proactive and largely automated
- Cyber power is 'Offence Dominant' and demands complete synergy. It must be so deployed

In the light of above-stated considerations, the task force studied existing cybersecurity architecture, the gaps by way of strategic deficiencies, level of integration with other instruments of power, organisation at the national level and the cyber readiness of our armed forces. The conclusion was that while the awareness, resources, organisation and limited infrastructure for cybersecurity existed on the ground and some activities were being undertaken, there was a glaring gap in the cyber power capabilities of our defence forces. Given the threats and the digitised battlefield, it is a strategic deficiency that could seriously impact our national security and therefore needs to be addressed urgently in 'Mission' mode.

The situation is time critical. We have to promulgate our cyber doctrine and build capabilities, which in view of galloping technology and related threats will remain a 'work in progress'. The task force has taken a roadmap of three years and hopes that alterations, enhancements and revisions would be done through constant monitoring to keep them relevant.

Indian Armed Forces Cyber Doctrine

Application of cyber power either on its own or in conjunction with other constituents of power will be decided by the CCS keeping in mind the overall threat scenario, the impact on national security and response needed to

a given situation. The task force recommends that the following situations would warrant use of cyber power either by itself or integrated with other instruments of power:

- Any cyber intervention which adversely impacts the availability of India's critical information infrastructure would attract a punitive response through conventional military means, including use of cyber power
- Any cyber probing mission resulting in loss of a platform, manned or autonomous, will be considered as an act of war and attract a response accordingly
- Exfiltration of sensitive information having an adverse effect on the economy, financial system, defence, security, atomic infrastructure and strategic industry would draw a strong and focused response in whatever manner India deems fit

For the purpose of cyber deterrence and application of cyber power, both civil and military assets would be considered as one. However, subsequent to clearance by the nominated authority, the conduct of cyber offensive operations and cyber deception would be the prerogative of the armed forces.

In view of the above, the Indian Armed Forces Cyber Doctrine would be:

'Multi-layer Resilience with Active Defence and Deterrence'

or

'Defence in Depth, Active Defence and Deterrence'

Defence in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise ... Defence in depth minimises the probability that the efforts of malicious hackers will succeed.

Active Cyber Defence (ACD) means acting in anticipation to oppose an attack involving computers and networks. Cyberattacks can be launched to repel an attack (active defence) or to support the operational action.

This doctrine would form the basis for developing full spectrum cyber power in the armed forces which would comprise of cyber-crime investigation including cyber forensic, counter cyber terror operations, cyber espionage, cyber defence in depth with particular emphasis on platforms, cyber offensive, cyber deception and cyberwar, either by itself or in conjunction with EW and kinetic means.

Development of processes and capabilities for employment of cyber power in different operations and training of cyber leaders must be the top priority. While areas of responsibilities between the civil authorities and armed forces must be defined clearly, the absolute necessity of information exchange, integration of capabilities, joint training and development of mission-oriented cyber weapons and so on should be emphasised clearly.

Organisation and Adaptation of Cyber Force

A dedicated organisation tasked with the raising and operationalisation of DCyA, suitably empowered and with assured budgetary support would be central to building requisite

capabilities. The implementation would be done in two parts concurrently and monitored by the COSC periodically.

In Part 1, we would enhance the capabilities at each Service and raise DCyA as an umbrella organisation responsible for training, equipping, fielding, infrastructure, integration and information management.

In Part 2, which would be implemented concurrently, we will recommend the methodology for integration of cyber power with cyber security architecture at the macro level, and command and control for ensuring least turbulence in implementation and yet be flexible enough to adjust to new threats and technologies.

The country needs to build thought leadership and weave together India's potential to create cyber power across the full spectrum under one organisation, empowered appropriately with complete responsibility, accountability and budgetary support.

One of the suggestions is to establish a National Cyber Security Commission (NCSC) – a fully empowered body under the Prime Minister, with its own department, on the lines of the Space Commission and the Atomic Energy Commission. Headed by a minister rank person, it would have two operational heads, one to handle the civilian aspect i.e., cyber security and the other who would be responsible for development and exercise of cyber power by the armed forces.

At the macro level, the NCSC would carry out requisite organisation transformation and be responsible for 'Adaptation of Cyber Forces'.

Human Resource, Training and Certification

The exercise of cyber power is dependent entirely on the skills of the operator at the tactical level as he is the 'man behind the gun'. At the operational and strategic level, we need cyber leaders adept in planning and conducting of cyber operations, both in standalone and integrated applications, in conjunction with IW and kinetic power.

This is an extremely critical area. The NCSP-2013 had set the aim of producing 500,000 cybersecurity Experts in next five years (2018). Presently, according one of the estimate there are only 1,50,000 such experts. There is an additional demand of half a million people with requisite skills.

A very tall order but doable with innovation and out of the box approach, change of working culture, attractive provisions with regard to pay and allowances, creation of an appropriate cadre with multiple avenues for growth, promotion channels, recognition and status backed by concentrated training, acquisition of skills and chance of location across the globe.

The armed forces must ensure 100 percent computer literacy in the next three years which must include 'Good Practices' and 'Cyber Hygiene' to be followed by all. Computer awareness, literacy and aptitude must be reflected in the appraisal which could form the basis of re-training and selection of cyber warriors.

Availability of cyber warriors and cyber leaders across multiple skills which constitutes cyber power is an extremely critical factor and perhaps the biggest challenge. The

armed forces will have to adopt a multi-level approach and concurrent execution. Following may be considered:

- Establish world-class training facilities along with the industry and academia to impart training with curricula for different levels and highly qualified faculty
- Select/recruit younger jawans/sailors/airmen with necessary qualifications and aptitude for ICT and computers and put them through a rigorous training capsule of three to four months designed by experts to concentrate on Computer Network Defence (CND). The brightest amongst these should be listed for training in Computer Network Attack (CNA) after a tenure of two years in the field. This training could be outsourced to corporate or academic establishments. A number of such courses can be conducted simultaneously on a zone/region basis
- While we must exercise this option of outsourcing, the armed forces must have training facilities of their own to impart military training and system integration with IW and KE assets
- Select limited batches of M.Tech. qualified officers and send them to different countries like Israel, UK, USA, South Korea, and Russia for training in different aspects of cyber warfare, participate in field exercises and develop processes and drills for employment of cyber power in the Indian context. These officers will form the nucleus in accordance with the concept of 'Train the Trainers'. They will also form the backbone of cyber leaders
- Multi-level cyber security should be introduced as a topic for graduation, postgraduate and doctoral studies in the Indian academic institutions
- Special care and emphasis must be given to select people for Computer Network Exploitation (CNE). They must be trained specifically in different languages, information assurance, big data, analytics, correlation, AI, cryptanalysis, code breaking, blockchain, analysis of 'kill switches', patch management, network management systems and designing of both disruptive and destructive cyber weapons
- Emphasis must be on correct recruitment, training, retention and re-training. Rules must be flexible and focused on attracting requisite resource. Some degree of relaxation in regimentation and working environment would be in order
- An extremely important aspect of training would be the development of an offensive spirit, the agility of mind and mental robustness to withstand cognitive attacks aimed at behavioural change, perception management and lowering of morale
- Explore organisations like NCC, NSS, ACC, and Police Cadets to provide young, motivated and disciplined resource for recruitment in the Cyber Warrior cadre. All these organisations must have cyber wings which would be a nursery to meet partially the requirements of cyber operators and cyber warriors

- Raise at least one Territorial Regiment in each Command capable of conducting all types of cyber operations, particularly CND and counteroffensive and detaching Integrated Teams in support of operations
- The launch of cyber offensive and cyber deception would be the responsibility of the Cyber Formation. Accordingly, at least 10 integrated teams will be created in three years on an incremental basis
- As part of 'Crowd Sourcing', create an organisation like 'Institute of Cybersecurity Professionals', select a highly qualified resource from corporate, academia and R&D establishments 'on call' to assist during crises. Initially, they could be invited to contribute in the formulation of strategy and assist in the capability build up
- Involve Indian diaspora for technology, training, investments and setting up R&D facilities
- The armed forces must immediately establish an **Academy of Information Operations and Management** with dedicated wings and facilities for training in the employment of cyber power across the full spectrum. This must be independent of training facilities of the Services and must concentrate on advanced training and strategy with requisite participation of the civil sector both in the faculty and as trainees.

Technology, R&D, Standards and Integrity of Data

As far as cyber security and cyber power are concerned, the absence of network technology, products and systems, electronic manufacturing industry, Indian standards for secure products, foundry for producing chips; limited crypto and cryptanalysis capabilities and very limited resource for system integration are some of the strategic deficiencies with a direct impact on India's 'Technological Sovereignty' and present serious vulnerabilities as far as cyber power is concerned. These are essential and fundamental pre-requisites for cyber power and need immediate attention.

Some of the major deficiencies were to be addressed by the implementation of the National Electronic Policy (NEP) – 2012. The policy needed to be revised in the light of a push under the 'Make in India' programme and integrated to meet the requirements of both cyber security and cyber power and made more attractive for people ready to invest.

The policy must concentrate on production of secure products and systems, their integration with expertise in 'engineering to production', based on Indian standards for information security and secure products, which are about to be released. Special emphasis must be put on the design and availability of 'secure industrial control systems'.

Given the fact that semiconductor chip manufacturing foundries are very capital intensive with still longer gestation period, it may be a good idea to hire the facilities abroad in the interim. That would compress the time frame for development of skills and be cost-effective, while concurrently, we establish own

facilities. This approach would mitigate the risks due to supply chain vulnerabilities to a large extent, especially in case of critical systems.

India being the fastest growing Internet and smartphone market carries substantial clout. She must use that for getting favourable terms with regard to the integrity of chips, the responsibility of the supplier in case of malware, cyber insurance and fastest delivery of patches/kill switches with a penalty for delays and setting up joint inspection facilities for chips, products and systems.

These should be an integral part of the contract document and would be easier to incorporate if manufacturing is being done in India.

Energise the 'Make in India' programme and encourage start-ups and SMEs to work on secure software, products and systems. Some of them have done well, exported their products and established joint ventures. Military orientation in these cases should be relatively easy and must be explored.

A formal military-industry interface and its association with design and manufacturing agencies is necessary.

We must have a WESEE-like organisation in all three services to start with and later in selected commands.

Integrated Teams must carry out a regular audit of platforms, weapons, systems and software to find vulnerabilities and how to close those. The manufacturer must be made an equal partner through a well-drawn contract and be responsible for 'availability' of systems, regular inspection for malware and release of patches to nullify any vulnerability or accommodate change in technology.

It is for consideration if an 'Inspector General, Cybersecurity' should be appointed with a small team of experts like Directorate of Air Staff Inspection (DASI) of the Indian Air Force, to oversee cybersecurity of platforms and weapon systems during peace and field exercises.

R&D for Secure Products Development and Cyber Weapons

India needs focused R&D in the development of safe products, discovery and analysis of vulnerabilities, fixing attribution, the design of 'kill switches' and security patches, creation and analysis of malware, production and delivery of cyber weapons; and concentrate on capability building for electronic combat as part of IW.

The Indian Armed Forces must have the most modern means and capabilities for cyber exploitation, technical intelligence, cyber deception and launching of probing attacks. In addition, depending on the knowledge of vulnerabilities, it must develop cyber weapons both for causing disruption and destruction. This necessitates R&D efforts in the development of critical technologies and their engineering into production.

Sharing of intelligence between the civil and military as also the launch of cyber weapons if the situation warrants, is a must and should be ensured through a statute if necessary.

Ensuring correctness of information and integrity of data are absolutely critical requirements along with regular surveillance for any 'Insider Threat' of sabotage, stealing technology or exfiltration of data.

Policy should be clear about options and methodology for the acquisition of technology which should include R&D, manufacturing, and availability of human resource with requisite skills.

There is urgent requirement for infrastructure like a cyber range, networks for simulation and making of cyber weapons.

Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence

Key facets of any military operation, particularly in the digitised battlefield of today, are intelligence, sharing of information, synchronisation and integration of various elements of combat power so that their effects complement and reinforce each other to achieve a quick and decisive victory with least cost to life and material.

The current generation of warfare supports information operations and is characterised by a blurring of lines between war and politics, combatants and civilians. Simply put, it is a war in which one of the major participants may not be a state, but rather a violent non-state actor or non-state actor sponsored by a state.

Conceptually, joint and integrated operations imply enunciation of the 'ways and means' of conducting Integrated and Joint actions with a singular aim of synergising and enhancing the warfighting capability of joint service components.

'Integration' in contemporary military matters implies integration of 'processes' across all operational domains of land, air,

maritime, cyberspace and outer space, towards optimisation of costs and enhancing readiness. It does not imply physical integration.

The foremost task of Cyber Formation/DCyA would be to ensure that integration is embodied across all functions – operations, intelligence, technology management, perspective plans, logistics, and human resource development (HRD). Such an embodiment enables common understanding leading to efficient and optimised responses.

Cyber Formation/DCyA would also jointly formulate processes for collaboration with the diplomatic, economic and information instruments of the national power, at all levels – strategic, operational and tactical.

An integrated approach comprising proactive engagement and shared understanding would be developed to bring distinct professional, technical and cultural disciplines of entities and sub-entities together.

The capacity buildup of cyber power would depend on what are appropriate mission sets, targets and spheres for operations. Based on these, the armed forces will work out tactics, techniques, procedures and authorities in cyber space for military operations.

Application of cyber power is generally done in four areas namely intelligence, technology, logistics (human resource with requisite skills, training, training infrastructure) and command and control. It is a 24/7 activity carried out in the following manner, namely:

- Business as usual – defacing websites, disruption and denial

- Information Operations – cyber espionage, social engineering, perception management (Mainly Disruptive)
- Attack on Critical Information Infrastructure (CII) and information assets (Destructive)

While cyber logistics has emerged as a new field requiring expertise and attention, cyber deception is an essential capability in cyber warfare.

‘Electronic combat’ with integration of CNO, EW and EM Spectrum has taken IW to a new level and has provided unique capability focused on the exploitation of asymmetry.

International Engagement and Legal Framework

Nature and characteristics of cyber space demands international cooperation by way of exchange of information, technology development, training and an appropriate legal framework to ensure cyber security and the right of safe navigation and passage in cyber space.

While India has signed several bilateral, regional and multilateral agreements for cooperation in cyber space, special efforts would be required for armed forces training, participation in exercises, military diplomacy, sharing of information of military value, joint development of technology and a common voice in the formulation of laws/policies. Such agreements with friendly countries can help ‘leap ahead’ in capacity building and hence must be given impetus at the highest level. The positioning of cyber experts in our missions abroad is strongly recommended.

The armed forces must have resources for cyber forensic and investigation of cyber-crimes. These could be add-on resources in the current legal department of the Services. Leaders must be conversant with the IT Act 2000 as amended in 2008. They also should be aware of the organisation for Internet Governance, ICANN, Tallinn Manuals and UN laws/deliberations on cyber war and cyber interventions.

As far as the budget is concerned, one can only make some assumptions. A ballpark figure of 6,000 crores over three years exclusively for capacity building of cyber power in the armed forces may be considered as the budget estimate. What is important and not negotiable is the assurance of availability of finance from the highest political authority.

Each Service must ensure availability of cyber qualified resource at the unit/ship/squadron level under a nominated Cyber Security Officer/Chief Information Security Officer (CSO/CISO), chartered with responsibilities for training, creating general awareness, information assurance, regular monitoring of possible threats, readiness of the establishment for cyber resilience measures and ensuring that cyber hygiene and other good practices are complied with at all levels.

Section Four

Organisation for Cyber Deterrence, Synergy, Staffing and Adaptation of Cyber Force

The organisation involves the provision of dedicated and appropriately skilled human resource, infrastructure, training and necessary equipment/systems in accordance with the policy and doctrine. In short, it implies the establishment of a cyber power eco-system.

While each Service has established some capabilities, there are no guidelines or policy formulation. Resultantly, an integrated approach is lacking. There is a lack of synergy, transparency and organised development of cyber power. The organisation is fragmented because of ambiguous command and control, and therefore, there is ad-hoc responsibility and accountability.

There is an acute shortage and uncertainty of finance, with each Service fighting for their perceived share. There is very limited interaction amongst the Services, both at the working and policymaking levels. Exchange of information is not formalised, thereby, defeating the basic tenet of synergy essential for cyber resilience. There is a shortage of skilled manpower, training facilities, system integrators and cyber leaders.

The first and foremost task of the Cyber Formation/DCyA would be to release a document detailing the cyber power eco-system for the armed forces, capacity building in each Service and integration at DCyA headquarters.

The DCyA would coordinate, issue necessary policies, ensure creation of suitably empowered and integrated organisations on the ground, the release of funds, availability of skilled manpower and training infrastructure.

These organisations must have government sanction to facilitate cyber

logistics development and infrastructure for training, besides establishment of laboratories and release of funds.

The task force recommendation is based on policies and processes promulgated by the Cyber Formation/DCyA, wherein, each Service provides resources, manpower, basic training, including infrastructure and logistics, for capacity building to provide necessary resilience against threats envisaged.

There is an urgent requirement of creating awareness of cyber threats, their impact on all areas of our existence and the ability of cyber weapons to cause disruption and destruction almost equivalent to WMD (mentioned above). Commanders have to be sensitised to threats in the digital domain. They must overcome misconception with regard to cyber power being 'technical' and concentrate on development of cyber power and its application for cyber resilience and offensive operations

Formation and unit commanders/ equivalent must ensure that the work and responsibilities of cyber personnel are given due importance and recognition they deserve and that they are dealt with professional dignity at par with other fighters.

Each Service must ensure availability of cyber-qualified resource at the unit/ ship/squadron level under a nominated Cybersecurity Officer/Chief Information Security Office (CSO/CISO)), chartered with responsibilities for training, creating general awareness, information assurance, regular monitoring of possible threats, readiness of the establishment for cyber resilience measures and ensuring that activities as part of cyber hygiene and good practices

are in order and complied with at all levels (mentioned above).

Special attention must be given to the use of social media and look out for any 'insider threat' during the periodic, but random audit. Surprise audits and checks must be instituted by the empowered team from the respective Service Headquarters/DCyA.

DCyA must formulate parameters for measuring a 'Cyber Security Index' (CSI) of a unit/organisation and communicate the same to all concerned. Measurement of CSI will be part of the annual inspection of the establishment. A score below the required threshold will invite special measures to be indicated by the DCyA.

Each Service Headquarters will ensure that necessary training and infrastructure are available for the men to prepare for Certification Tests to be conducted by DCyA or other nominated agency.

Cross-domain training and exercises involving persons from each Service and DCyA must be done regularly. Actions to obviate the flaws, particularly related to the discovery of vulnerabilities must be undertaken on top priority and a record maintained. All concerned must be informed and data be maintained in the nominated data centre, thus ensuring its integrity.

There is a strategic, inescapable and urgent requirement of a 'Directorate of Information Assurance and Management' to be formed immediately at the tri-service level with its nodes at each formation/equivalent connected with fully secure and high-speed data links connected further with the data centres established by each Service.

Institute a Cyber Cadre with immediate effect with flexible construct and less regimentation.

Tap organisations like NCC, ACC, NSS and Police Cadets for getting younger, disciplined and motivated resource.

As part of intelligence acquisition and monitoring, recruit requisite resource to operate in and monitor dark web and deep web. This capability and task could be given to Military Intelligence and other intelligence set ups at the appropriate level.

Recruit, train and deploy 'cyber modules' and 'lone wolf' operatives for strategic intelligence and special tasks.

As part of 'crowd sourcing' raise a special TA unit consisting of experts in cyber-related skills. They can be deployed on special tasks and as part of crisis management either directly or as part of concerned CERT.

Create an 'Institute of Cyber Professionals' to draw volunteers and as a possible resource for CND and CNA tasks.

Organisation for Capacity Building in Cyber Deterrence

Indian Army

A quick analysis of the role, equipment profile and human resource of the three Services would show that the army's major vulnerabilities lie in its manpower and the C4ISR assets, including sensors and to an extent in weapon platforms. The adversary will make efforts to collect intelligence by all means like HUMINT, ELINT, SIGINT, MASINT, OPSEC and OSINT with the aim of attacks

in cognitive and Electronic Warfare (EW) domains. These present a strong challenge to our defences.

The organisation must have capabilities to be able to handle adversary's efforts in EW, perception management and attempts to change human behaviour by cognitive warfare. Also, connectivity from sensors to shooters as indeed the working of sensors and weapons themselves must be ensured through resilient networks, regular hardware and software maintenance and highly skilled manpower to maintain fighting potential and avoid the feeling of isolation for that would aid cognitive attacks.

Such a scenario dictates that the army must be organised, equipped and trained for Information Warfare and must have integral capabilities to thwart electronic/cyber interventions, launch offensive operations at the tactical level and provide a launch pad to DCyA teams for offensive CNO.

The Indian Army needs to balance its obsession with kinetic energy systems with the absolute necessity of ways and means for 'Electronic Combat' (IW+EW+EM Space) for that is the most likely threat that manifests 24/7.

The task force recommends that necessary measures for ensuring CND should be available at all levels of command and integrated cyber, IO and EW organisation at the formation level. Information Warfare brigades with specialised units in the cyber domain, EW and IO should be on the 'Order of Battle' of a Corps to begin with.

Indian Navy

India has a vibrant Blue Economy based upon maritime trade, mercantile marine vessels, port activity, offshore oil and natural gas exploration and associated networks of evacuation pipelines, undersea communications cables and so on. Peninsular India's vast coastline is dotted with 12 major and over 200 other ports. It has an Exclusive Economic Zone of over 2,172 lakh square kilometres. All these national maritime assets require protection from interference during peace and during hostilities. These fall into two distinct classes:

(a) Civilian/economic and

(b) Military, i.e., Navy and Coast Guard

Civilian/Economic Maritime Assets. The International Maritime Organisation (IMO) has promulgated a series of advisories containing guidelines for cyber security, the most significant and comprehensive ones being Guidelines on Maritime Cyber Risk Assessment (5 July 2017) and Guidelines on Cybersecurity on Board Ships (December 2017). Their implementation on all vessels flying the Indian flag must be ensured and audited periodically by a dedicated and empowered organisation.

Navy and Coast Guard Assets. Exclusive Navy and Coast Guard seagoing and shore-based assets including ships, aircraft, submarines, harbours, dockyards, air bases, refuelling facilities, armament and stores depots, shore-based surveillance and coastal defence weapons all need to be protected from cyber intervention by state and non-state actors who not only seek to disrupt the national economy but also to degrade the

fighting capability of naval warfighting assets of all kinds.

Organisational and technical arrangements must be in place separately for civilian and military requirements up to a certain level, beyond which they must grow into a congruence at the top of a pyramidal maritime cyber security hierarchy.

Distinct Roles for Indian Navy

The Indian Navy would have overall responsibility for maritime cyber defence in its area of jurisdiction and would provide a firm base for cyber offensive operations to the DCyA.

An empowered Coast Guard would be responsible for cyber defence of all shore establishments and for periodic audit of compliance with standards, policies and processes issued by DCyA and Naval Headquarters. The status and non-compliance will be reported to the DCyA and Naval Headquarters.

Proposed Organisational Hierarchy

Cyber Formation/Defence Cyber Agency would be the apex body to oversee all aspects of capacity building of cyber power for the maritime domain in coordination with established institutions such as NSCS, CERT, NTRO and NCIIPC.

The National Maritime Cyber Operations Centre (NMCO) would be the coordination centre for cyber operations within the Navy and Coast Guard and with other services. The CERT-Navy and its Cyber QRTs would be part of it.

The Indian Navy's Cyber Agency and the Indian Coast Guard's Cyber Agency would be responsible for implementation of the Action Plan, including training and maintaining skilled manpower, inspection and enforcement of maritime cyber security standards and providing respective CERTs and Cyber QRTs.

There would be corresponding cyber security professionally manned billets at the levels of Navy Command and Fleet Headquarters, and at Regional Coast Guard Commands. These organisations would also have designated Command-level CERTs, appropriately trained and staffed.

The WESEE would develop cyber expertise to become the technical cyber advisor to develop the cyber-secure framework, including for Internet of Things (IoT) and issue relevant guidelines for implementation and inspection of cyber-secure naval equipment, including naval propulsion and engine control systems.

WESEE would guide the Director General of Naval Design (DGND) on design, inspection, development, manufacture, installation of connected onboard sensors and weapons of all naval vessels i.e., from design to delivery and subsequent operationalisation. WESEE would provide this service to the Coast Guard also.

Shipboard Cyber Expertise

While the Navy must have a dedicated Chief Information Security Officer on board, as an interim measure, the skill set of the officer looking after Communications and EW should be enhanced to include all aspects of cyber security and applications of cyber power.

Skill Development

Skills required for capacity building in cyber power are multi-fold with a very high degree of specialisation. The Navy would formulate curricula for each skill and ensure availability of infrastructure and faculty, as also ensure facilities for certification are available. Most of the training could be outsourced. Integral establishments of the Navy like the Signal School, INS Valsura and Submarine and Naval Aviation Training School should be organised and equipped for military training and application of cyber power.

An annual seminar on maritime cyber security should be organised by the National Maritime Foundation on the sidelines of one their annual conferences.

Designated teams need to be sent to various countries for interaction and learning.

Study courses should be organised in foreign universities having expertise in maritime cyber security.

The Navy must have its own cyber range, data centres, network simulators, incident reporting network, and facilities for software maintenance and inspection.

Periodical Inspections of Naval and Coast Guard establishments must include specialist cyber professionals to review cyber awareness, incident reporting and response mechanisms.

International Cooperation

It is necessary to interact with international maritime organisations who have already developed expertise in maritime cyber security. Some of them are IMO, US Coast

Guard and GCHQ. It should also be noted that India has entered into cyber security related agreements with countries like the USA, UK and Israel. These connections should be leveraged to our advantage to 'leap ahead' and save time.

Indian Air Force

The Indian Air Force (IAF) has had an extensive cyber security policy in place since 2007. This was revised in 2012 and 2018. Treated as a Bible in the Service, this cyber security policy covers the entire gamut of cyber activity, be it AFNET or Internet or LAN or weapon systems. It discusses in detail the various procedures to be adopted in IAF cyberspace. To augment the Cybersecurity policy, various Cybersecurity instructions and advisories are issued from time to time to ensure the Cybersecurity posture of IAF remains relevant with respect to both the technology and emerging threats.

The IAF has done some pioneering work in cyber defence, offence, information management and created organisations for audit, training and for separating the Internet from AFNET.

The interaction between AFNET and Internet is carried out through a Centralised Internet Access Server which is managed in turn by the Internet Security Operations Center. The IAF has developed its own operating system 'Vayusenix'. CERT-IAF conducts regular audits, and is responsible for 'Patch Management' and works directly under the Directorate of Operations (IW) which is the apex policymaking body for any cyber security related issue and is functionally under the Assistant Chief of Air

Staff Operations and Space, who is also the Chief Information Security Officer (CISO) of the IAF. Air Commodore Ops (IEW) is the overall in-charge of the Directorate for its day-to-day operations.

Command Headquarters plays a crucial role in cyber defensive operations in the Area of Responsibility (AoR) of the concerned Command. Command Information Warfare Officer (CIWO) is responsible for ensuring effective implementation of the cyber security policy and the directives issued by Air Headquarters. CIWO also plays a crucial role in carrying out routine and surprise checks of cyber security units at air force stations.

The Indian Air Force takes cyber audits of its ICT infrastructure very seriously. There are various kinds of audits, varying in role and complexities to evaluate different systems. It includes audit of Critical Information Infrastructures (CII), weapon systems and platforms, Headquarters at all levels, air force bases, logistic organisation and so on. The audit also includes Vulnerability Assessment and Penetration Testing (VAPT) and surprise audits. The IAF also carries out an audit of personal ICT devices of Air Warriors on a voluntary basis to protect them from cyber interventions.

Impediments to Cyber Security

There are certain procedural impediments which have a direct impact on capacity building of cyber power and national security which must be resolved at the earliest. Some of these are:

- Cyber security organisations viz., Dte of Ops (IW), CERT-IAF, iSOC, SOC and certain appointments viz., CIWO/

SIWO are not established under the government gazette

- With no sanction for an establishment, manpower for running these organisations is not available on accretion basis. The manpower for these key roles is arranged from within resources on an ad-hoc basis
- Ad-hoc manpower may be routed back to the parent branch/trade. This results in a skill drain, as the trained and experienced resource is not available after being routed back to the parent trade
- Sans establishment, the IAF faces certain bottlenecks in undertaking capital works viz., Work Services for creating Cyber Ranges, Cyber Laboratories etc.
- Non-availability of establishment also hampers the procurement process. There is crucial software (Forensics, SIEM etc.) that could not be purchased on time
- The Forensics Lab is to be certified and recognised by Indian courts for an early trial of cyber-related cases

Defence Information Assurance and Research Agency (DIARA)

To begin with, DIARA will form the nucleus of the Cyber Defence Agency (DCyA) and ultimately merge with it. Hence the way the Defence Cyber Agency comes up will be contingent and dependent on the involvement, functioning, organisation and empowerment of DIARA, the support and guidance that it receives from the government, the Chiefs of Staff Committee and the National Cybersecurity Coordinator.

Following are indisputable and absolute strategic imperatives in the creation and operationalisation of DCyA:

- Immediate government letter sanctioning formation of the Defence Cyber Agency, its approved organisation with incremental manpower, the Command and Control and Delegation of Powers to the Commander DCyA
- The government letter must include approval in principle for location and infrastructure – buildings for offices, conference and meeting rooms, communication hub, data centre, cyber range, laboratories; and access control system to include the latest security systems. Some of these assets would require shielding from Electro Magnetic Interference
- Budget allocation of 2,000 crores with a provision to carry over the balance to the next financial year, financial sanctioning power of 20 crores with the Commander and 100 crores with the approval of the integrated finance officer and the Steering Committee
- A Steering Committee, duly empowered, headed by the CISC and having Members as stakeholders, be formed by issuing appropriate government letter. The Steering Committee would report to the Raksha Mantri and be responsible and accountable for timely implementation and operationalisation of DCyA. Slippage of eight weeks or more to be brought to the notice of the PM/PMO, NSA, COSC and NCSC clearly stating the reasons and recommended solutions
- Nominate a think tank with requisite domain knowledge and experience as a consulting agency for compressing time frame and creation of knowledge through analysis of technical developments and their utility in the Indian context, emerging threats, and locating human resource
- DCyA should have a younger profile, flexible policies about tenure, promotions and cadre management. Merit must be respected, acknowledged and rewarded. Selection should involve tests for aptitude, security consciousness, out of the box and innovative thinking and the 'never say die' spirit
- DCyA must have different departments and supporting facilities for human resource, training and certification; technology and R&D; intelligence, cryptology, coding, language, networks and sensors; safe products and systems; policies, processes and battle drills; integration, military diplomacy, international cooperation; and interaction with cyber security components in the civil, including joint exercises
- In the first year, DCyA should be able to provide a minimum of Two integrated teams which must be operational in 18 months. Thereafter, in the second year, capacity must be built for Three integrated teams, and for Five integrated teams in the third year. Needless to say the teams would be constituted, based on the task, and hence will have a very flexible construct
- Operational parameters, particularly for command and control of these teams and the integral elements, would get formulated as we go on

Human resource in the IT sector in general and cyber security experts in particular is not prone to a long chain of rigid hierarchies. They work in flat organisations driven by the concept of 'knowledge worker'. Their organisational culture inculcates and encourages interdisciplinary cooperation, seamless flow of information, honesty and integrity in reporting and ownership of responsibilities. Members in the organisation have to be creative, innovative and keen to learn from each other's experience. We must recognise these cultural attributes and formulate specific HR policies and terms of engagement for this highly technical and limited resource.

Section Five

Human Resource, Training and Certification

The efficacy and application of cyber power is contingent upon human resource, their skills and level of competence. Unfortunately, there is an extreme shortage and availability of resource. Getting the right people is most critical and a top priority for any organisation. Next in priority is training, retention and re-skilling.

The task before cyber power operators is highly specialised and demanding. Hence keeping them motivated is a big challenge. This is particularly so since the working culture and attitude does not lend itself to regimentation. Further, they are quite aware of their expertise and the enormous demand in the civil sector for their services, and hence the expectation for higher emoluments, career progression, dignity and recognition. Unfortunately, these come with great difficulty due to a distinct bias against 'techies' in the Services. The challenge, therefore, is two-fold – first to keep them motivated, and second, to make the environment aware about the importance of their task and how it adds another option to warfighting and in delivery of un-proportionate dividends.

Another challenge in terms of recruiting and retaining technically qualified individuals is that the skill set of an expert hacker is the same as those of a cyber security/ICT expert. Such skilled persons are in great demand, both in industry and Dark Web and are well compensated.

The domain where this human resource will perform is the new global called 'cyberspace' which is an integrated civilian and armed forces domain. This paper deals with capacity building of cyber power in the Indian Armed Forces. Hence, the major area of its application could be called 'Military Cyber Space' for better understanding – a

theoretical subset of cyberspace, which includes relevant linkages with non-military cyberspace, wherever necessary.

Military cyberspace will include all networks, communications and data centres specifically used by the military in isolation from non-military users. It includes the electromagnetic space, including EM Spectrum, C4ISR assets, weapon platforms (aircrafts, ships, maritime assets, tanks, drones, missiles, logistics elements, networked soldiers in combat), and social media networks in the area of interest and influence, and digitised national media reporting on military activities and so on.

The sole aim of defining military cyberspace is to highlight the complexities of the operational environment in which a cyber warrior must operate, the multitude of skills required to effectively deliver and integrate with other warfighting domains.

Human resource in the IT sector in general and cyber security experts in particular is not prone to a long chain of rigid hierarchies. They work in a flat organisation driven by the concept of the 'knowledge worker'. Their organisational culture inculcates and encourages interdisciplinary cooperation, a seamless flow of information, honesty and integrity in reporting and ownership of responsibilities. Members in the organisation have to be creative, innovative and keen to learn from their experience. We must recognise these cultural attributes and formulate specific HR policies and terms of engagement for this highly technical and limited resource.

The situation can be eased considerably by outsourcing training to the private sector.

They can deploy domain specialists, hardware and software in a much faster time frame than is possible through normal defence procurement procedures. The curricula can be drawn jointly by the armed forces and private enterprise. Aspects of security of information and Intellectual Property Rights (IPR) can be resolved through a well-drawn contract with comprehensive and stringent non-disclosure components. Such a measure will be a catalyst in building a cybersecurity eco-system.

The situation is critical and needs to be dealt with at multiple levels concurrently.

The government must declare cyber security as a separate cadre immediately, as there is a strategic necessity to develop an eco-system to generate skilled human resources.

At the national level, all academic institutions must be directed to include basic cyber security training as part of their curricula. The armed forces should identify academic institutions for training in different skills up to advanced and doctorate levels. The selected institutions must be given grants for establishing training facilities and employing qualified faculty. The selected people should be sent abroad for specialised training.

Organisations like the NCC, NSS and Police Cadets must have cyber wings and become a nursery for skilled resource, both for the civil and armed forces.

An Institute of Cyber Professionals must be formed to draw skilled and experienced resource, both from within the country and abroad.

All stations must be directed to form cyber orientation clubs, which will be open to

families of the armed forces personnel, both to create awareness and for talent hunting.

Focus Area of Securing Military Cyber Space

As far as the armed forces are concerned, capacity building focus would be on identifying and protecting vulnerabilities in the military cyber space, create escalating levels of expertise for cyber security, high level of multidisciplinary expertise for deterrent capability and developing advance knowledge for the future.

The primary thrust of training will be in detection of threats, containment of damages and recovery from cyberattacks. While defensive capabilities will have their own place, specialised training to selected persons should be imparted in cyber offensive operations.

At the operational and strategic levels, we need cyber leaders who are adept in planning and can conduct cyber operations, both in standalone and integrated applications in conjunction with IW and kinetic power.

Some skills required for developing the full spectrum of cyber deterrence are: PC operating systems and exploits (*A computer exploit, or exploit, is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders. Used as a verb, exploit refers to the act of successfully making such an attack.*)

- Mobile operating systems and exploits
- Computer hardware and embedded devices
- Networking protocols, wired and wireless networks

- Switches, routers and wireless access points
- Firewalls and intrusion prevention systems
- Databases and memory operations
- Computer attack, exploitation and security
- Constructing and detecting malware
- Hacking tools and programming languages
- Internet architecture, Dark Net, Internet of Things and Open Source Intelligence (OSINT)
- Advanced exploits relying on assembly level programming, data execution prevention, address space layout mechanisms, function pointer overwrites, heap spraying, EMET mitigations, kernel hacking, etc.
- Language expertise
- Coding, code breaking, cryptology and cryptanalysis
- System integration, cyber deception
- Data storage and management, big data, AI, and analytics
- Electrical, electronic and civil engineering expertise
- Psychology and behaviour analysts

The task force recommends four levels of cyber proficiency in the armed forces. These are:

Level One: Cyber Literate

This level has two possible entrants – soldiers in service and those who are to be recruited. Both groups will be made cyberliterate up to Level 3 or 4 of the National

Skill Qualification Framework (NSQF). Training would be in accordance with a 'Qualification Pack' designed by the DCyA to cater for the specific needs of the armed forces. Stress will be laid on cyber hygiene, good practices, incident reporting and creating awareness of possible threats. A target of more than 90 percent persons becoming cyberliterate should be achieved within two years. Training would include refresher capsules conducted periodically to remain abreast with technology and emerging threats. All existing training institutions will be organised and equipped by way of faculty, infrastructure and finance for this task.

With regard to new recruitment, Level 3 qualification of NSQF must be the essential qualifying criterion. They would be given reorientation training by way of a Cyber Foundation Course as part of initial training in their respective institutions.

All Level 3 and 4 persons will be subjected to aptitude and psychometric tests (to be developed by DIPR) to ascertain their suitability for cyber roles and associated aspects like confidentiality. Those clearing this test would undergo an additional cyber capsule of approximately three months duration and conform to the next NSQF level.

Level 2: Cyber Operators

We need to understand that a cyber specialist needs to have a flexible mind and good insight into cyber/software/network aspects of relevant application and/or equipment that is inducted into the cadre. Cyber operators would form Level 2 with a minimum qualification of graduate or Level 5 to 9 of NSQF.

They will be sourced from those who qualify in the test mentioned above and through direct recruitment at a rank equivalent to that of a Junior Commissioned Officer (JCO). This resource will man and operate networks, systems and platforms. They would be specifically trained in software maintenance, cyber defence, vulnerability detection and resolution, security audits, network penetration and integration. They will form the backbone of cyber power capability. Cyber operators would be proficient in one or more of the skills stated above. Some of them can be embedded with equipment manufacturers to monitor and learn.

Level 3: Cyber Warriors

These are hardcore cyber experts in their respective fields with at least an engineering degree and minimum of three years of experience. They would be given tasks like cyber exploitation on 24/7 basis, identification of vulnerabilities, probing missions, information management, engineering inputs for cyber weapons, integration with kinetic energy assets; execute tasks assigned as a constituent of IW; design and data on kill switches; and so on. They would provide a firm base to DCyA integrated teams for offensive operations and also be able to conduct counter-offensive missions. The brightest amongst them will be sent abroad for specialised training and postings to Indian diplomatic missions.

Level 4: Cyber Leaders

These are highly qualified people with a Master's Degree or Ph.D. with five to seven years experience and an 'outstanding' career profile. They would be involved in policy

making and formulation of concepts of operations, both in the cyber-enabled tasks and in integration with other warfighting assets. They must be sent to friendly countries like the USA, UK, Russia, Israel and South Korea for specialised training in the field of their expertise. They would be in command of cyber units and be responsible for capacity building and application of cyber power. They would provide domain knowledge for India-specific research and development and interact with top academic institutions for the provision of faculty and talent hunting.

Some Other Issues

- There will be a requirement for setting up skilling institutes, some of them anonymous, to re-skill and up-skill personnel so that they stay updated and have adequate mobility and opportunities for career progression
- The functioning of these institutes should be entrusted to those personnel who undergo rigorous screening in terms of integrity, confidentiality and subject matter expertise
- Recommend setting up one cyber range per geography to conduct theatre aligned specialised courses
- Language training. Ensure availability of adequate vacancies and finance for language training
- Create a pool of Master Instructors to lead the training and be available for crisis management in case of a major cyber intervention
- Establish online training and a certification facility along with resource for content generation. Conduct

- military hackathons, competitions and awards to incentivise the seen face of the cyber workforce, both to attract fresh talent and to keep existing talent motivated.
- The unseen face will also have to be equally incentivised by non-public disclosures.

Conclusion

Human resource and related aspects of training, role, responsibilities, attitude and institutional values, coupled with innovation, agility of mind, motivation, out of the box thinking and unwavering belief in the

organisation would define a cyber warrior. It is a very scarce resource with several suitors to attract them with tempting terms of service. We, thus, have a challenge which demands a proactive approach with an attractive package, good working conditions, enabling policies, recognition as a separate cadre and dignity as a knowledge worker.

The armed forces will have to adapt to this environment and rely on years of management experience along with a study of human resource practices in the private sector.

Time is critical and there is no choice.

India has to develop its own technologies, electronic manufacturing base, R&D infrastructure and highly skilled human resource. Being late has an advantage of 'leap ahead' but delays can have catastrophic consequences also. There is a need to encourage our industry, provide a level-playing field at the minimum, encourage start-ups and MSMEs and create a vibrant eco-system.

Section Six

Technology, R&D, Standards and Integrity of Data

Introduction

Cyber security requires continuous tracking of evolving technologies globally and alignment with the country's R&D objectives and agenda. Contribution is required from all stakeholders – government, industry and academia. Public-Private Partnership (PPP) is the way forward, as it would help in combining the best of both worlds and complement capabilities to develop a secure cyber eco-system. Increased government-funded research and public-private coordination are needed, particularly in the expanding fields of new secure networking and computing architectures, high performance computing, encryption, data integrity, artificial intelligence, big data, privacy and risk management strategies.

Capability building in cyber power is essentially about the availability of appropriate technologies and their exploitation in achieving the desired effect. The availability of an indigenous technology base, its application in the development of products, integration in accordance with national standards to build systems and ensure interoperability coupled with indigenous semi-conductors, an electronic manufacturing and testing eco-system, focused R&D to support immediate requirements and concurrent work on harnessing futuristic technologies are critical strategic requirements for any nation in order to have 'Technology Sovereignty' and develop full spectrum capabilities in cyber power.

Unfortunately, India has a long way to go in these areas with attendant adverse impact on cyber and national security. We have to design, produce, integrate, field, maintain and upgrade fully secure indigenous products and systems as per Indian standards with

integrated circuit chips produced in India. Without these, India will continue to have serious and unacceptable vulnerabilities in her defence posture.

In this information age, information and technology are the new currencies of power. The nation must have capabilities and processes to ensure integrity of information through all stages, capture, transport, storage, processing and retransmission. There is an operational and strategic necessity to have indigenous capabilities in language, big data, analytics, artificial intelligence, cryptology and data centres with wide band secure connectivity.

Data is the new oil and we as a nation have to ensure that our data is stored in servers located in India. While the national data policy is likely to be announced soon, the government's stand on 'localisation of data' is praiseworthy.

Suggested Approach for Technology Development

India has to develop and harness indigenous technologies to back up her doctrine. India has the capability but needs political support, enabling policies, financial backing, and less bureaucratic control. India is a lead country in designing semiconductor chips but lacks a foundry for in-house production.

It is very heartening to know that India very recently, has produced a completely indigenous microprocessor, thanks to researchers from IIT Madras. The microprocessor can be used in mobile computing devices and embedded low power wireless and networking systems. The project named 'Shakti' is funded by the Ministry of Electronics and Information Technology. The manufacturing was done at

the semiconductor laboratory of ISRO. The first batch of 300 chips, known as RISECREEK, were fabricated at Intel's fabrication facility in the US.

Another project with SCCI collaboration has successfully created a new standard for cyber-physical systems design and development. This is perhaps the first time in the world that the world of models and realisations are fused into a single architectural continuum! This puts India at the forefront of digital and cyberphysical systems modelling standards efforts. Such architecture allows a new system to be modelled and automatically synthesised to a working system that is guaranteed to conform to the model, speeding up the entire development cycle.

These and many more 'islands of excellence' exist. We need to integrate them to create secure systems. We must encourage this and produce a qualified resource for 'engineering into production' and system integration. This should be one of the main R&D objectives.

The task force recommends multiple approaches to be implemented concurrently: Establish a 'National Mission for Information/Cybersecurity Technologies Development'. This should be headed by a technocrat and members drawn from stakeholders, including representatives from users, private industry, academia and R&D establishments

- Carry out a detailed study and analysis of present and emerging threats and home onto technologies that are needed with timelines for their development to support the doctrine

- Create/award dedicated 'projects' for the development of each technology, its transformation from engineering into production, integration and upgradation. These projects to be awarded to a consortium of companies/institutions in a PPP model with 'womb to tomb' commitment
- Timelines for implementation of each phase must be clearly specified with provision for penalty in case of slippage and incentives for early completion within the budget and innovations
- The Project Director/Lead Company will have complete responsibility and accountability. They would be suitably empowered and have assured access to financing
- Attractive provisions and incentives for start-ups and involvement of medium and small scale enterprise (MSSE)
- Ensuring availability of human resource and training facilities as given in the previous chapter
- Review/Revise National Electronic Policy-2012 and give it strong impetus
- Hire a foundry for semi-conductors from a friendly country and concurrently commence deliberation for a foundry in India

Cyber security is an integrated civilian and military domain. Hence, the technologies would be largely common, especially for defensive tasks. Some of these technologies, however, would have to be developed on higher priority to meet the immediate security requirements of the defence forces. For offensive operations, the making of cyber

weapons and deception, we might need some application-specific technologies.

Emerging Threats and Corresponding Negation Technologies

The old IT world is dying; cyber security experts now have to deal with threats created by Cloud, the Internet of Things, mobile/wireless and wearable technology. Data that was once contained within systems is now travelling through a dizzying variety of routers, data centres and hosts.

Today we are facing 5th Generation cyber security threats wherein, attacks are multi-everything – multidimensional, multi-stage, multi-vector and polymorphic. To properly protect a business's IT operations today requires a new, holistic approach to assessing and designing their security toward an integrated and unified security infrastructure that prevents attacks in real time.

From curious hackers to corporate and state-sponsored espionage to organised crime, the new networked world has provided near unimpeded access to all sorts of assets and private data with near complete anonymity! As a result, every successful advancement of malicious activity has driven corresponding advancements in IT security. This cycle will certainly continue.

What's more, cyber criminals and hackers are getting smarter. For instance, they are using:

- Man-in-the-Middle (MiM) attacks to eavesdrop on entire data conversations
- Spying software and Google Glass to track fingerprint movements on touch screens

- Memory-scraping malware on point-of-sale systems
- Bespoke attacks that steal specific data (instead of compromising an entire system)

In these scenarios, firewalls, anti-virus measures and tool-based security approaches no longer cut it. By 2020, it is predicted that 60 percent of digital businesses will suffer major service failures due to the IT security team's inability to manage digital risk in new technology and use cases.

New solutions are needed now.

Increasing digital connectivity and the automation of virtually all processes in the world of business throughout the whole value chain have led to the creation of agility. This has also led to the development of extremely high levels of threat and significantly raised cyber security risks. The building of cybersecurity into applications is critical in addressing such risks, as well as all the devices that are interconnected from the very beginning. As attackers improve their capabilities, enterprises must also improve their ability to protect access and protect from attacks. Security and risk leaders must evaluate and engage with the latest technologies to protect against advanced attacks, better enable digital business transformation and embrace new computing styles such as cloud, mobile and DevOps.'

Priority Technologies for Defence Forces

Cloud workload protection platforms and cloud access security brokers: The continued and growing significance of

software as a service (SaaS), combined with persistent concerns about security, privacy and compliance, continues to increase the urgency for control and visibility of cloud services.

Remote Browser: Nearly all successful attacks originate from the public Internet, and browser-based attacks are the leading source of attacks on users. Information security architects cannot stop attacks but can contain the damage by isolating end-user Internet browsing sessions from enterprise endpoints and networks.

By isolating the browsing function, malware is kept off of the end user's system and the enterprise significantly reduces the surface area for attack by shifting the risk of attack to the server sessions, which can be reset to a known good state during every new browsing session, a tab opened or URL accessed.

Deception: Deception technologies are defined by the use of deceptions, decoys and/or tricks designed to thwart or throw off an attacker's cognitive processes, disrupt an attacker's automation tools, delay an attacker's activities, or detect an attack. By using deception technology behind the enterprise firewall, enterprises can better detect attackers that have penetrated their defences with a high level of confidence in the events detected. Deception technology implementations now span multiple layers within the stack, including endpoint, network, application and data.

Endpoint detection and response: Endpoint detection and response (EDR) solutions augment traditional endpoint preventative controls such as an anti-virus by monitoring endpoints for indications of unusual behaviour and activities indicative of malicious intent.

Network traffic analysis: Network traffic analysis (NTA) solutions monitor network traffic, flows, connections and objects for behaviours indicative of malicious intent.

Managed detection and response: Managed detection and response (MDR) providers deliver services for buyers looking to improve their threat detection, incident response and continuous-monitoring capabilities but don't have the expertise or resources to do it on their own.

Micro-segmentation: Once attackers have gained a foothold in enterprise systems, they typically can move unimpeded laterally ('east/west') to other systems. Micro-segmentation is the process of implementing isolation and segmentation for security purposes within the virtual data centre. Like bulkheads in a submarine, micro-segmentation helps to limit the damage from a breach when it occurs.

Software-defined perimeters: A software-defined perimeter (SDP) defines a logical set of disparate, network-connected participants within a secure computing enclave.

Operational Support System (OSS) security scanning and software composition analysis for DevSecOps: Information security architects must be able to automatically incorporate security controls without manual configuration throughout a DevSecOps cycle in a way that is as transparent as possible to DevOps teams and doesn't impede DevOps agility but fulfils legal and regulatory compliance requirements as well as manages risk. Security controls must be capable of automation within DevOps tool chains in order to enable this objective. Software composition analysis (SCA) tools specifically analyse the source code, modules, frameworks and

libraries that a developer is using to identify and inventorise OSS components and to identify any known security vulnerabilities or licensing issues before the application is released into production. This is of special significance to India in case of imported equipment and systems.

Container security: Containers use a shared operating system (OS) model. An attack on a vulnerability in the host OS could lead to a compromise of all containers. They are not inherently insecure, but they are being deployed in an unsecured manner by developers, with little or no involvement from security teams and little guidance from security architects. Traditional network and host-based security solutions are blind to containers.

Hardware Authentication. Tech gurus have developed a solution in the user authentication process with a new Core vPro processor that belongs to the sixth generation of processors. The core vPro can combine different hardware components with enhanced factors simultaneously for user identity validation purposes.

Tech Company Intel has built on previous experiences and mistakes and dedicated a portion of the processor for security reasons to make a device part of the entire process of authentication. Hardware authentication can be especially important when it comes to the Internet of Things (IoT) where the network of connected devices ensures that any device that seeks to be connected has the rights for connectivity to that particular network. This is of immense value in hardening various network systems on board military platforms.

Deep Learning: Some technologies are encompassed in deep learning such as machine

learning and artificial intelligence. There is a significant deal of interest for purposes of systems security in these technologies.

Deep learning, just like behaviour analytics, focuses on anomalous behaviour. Whenever AI and machine learning systems are fed with the right data regarding potential systems security threats, they can make decisions on how to prevent hacks depending on their immediate environment without any human intervention.

The system scrutinises entities instead of users that have access to the information system. The most recent developments in machine learning technology and exact business analytics means that we are now able to analyse different entities that are found in the enterprise at both the macro and the micro levels. Business organisations and government agencies are now be able to stamp out any persistent or advanced cyber threats using artificial intelligence and machine learning.

In the past few years, hackers have been employing customised attacks on systems. Instead of launching a battalion at a wall, they carefully analyse a system's defences, and then send in the Trojan horse. Thanks to the volume, velocity and variety of big data, most companies are not even aware that their systems have been breached.

Instead of focusing on the first line of defence, the next-generation breach detection focuses on what happens once the criminal is inside the system. It takes behavioural analytics and adds even more tools to identify the bread crumbs that a hacker leaves behind.

Rather than relying on detecting known signatures, we can marry big data techniques

such as machine learning with deep cyber security expertise to profile and understand user and machine behaviour patterns, enabling them to detect this new breed of attacks. In other words, breach detection tools can pick out strange movements and changes in a sea of data and determine that something is very, very wrong.

Virtual Dispersive Networking (VDN): VDN takes a page out of now traditional military radio spread-spectrum security approaches, where radios rotate frequencies randomly or split up communications traffic into multiple streams so that only the receiving radio can reassemble them properly. With Dispersive, however, the Internet (or any network) is now the underlying communications platform.

VDN splits a message into multiple parts, encrypts each component separately and routes them over servers, computers and even mobile phones. Traditional bottlenecks can be completely avoided. The data also 'roll' dynamically to optimum paths – both randomising the paths the messages take while simultaneously taking into account congestion or other network issues. Hackers are left scrambling to find data parts as they whip through data centres, the Cloud, the Internet and so on. To prevent cyber criminals from attacking the weak point of the technology – the place 'where the two endpoints must connect to a switch in order to initiate their secure communications' – Dispersive has a hidden switch that also leverages VDN. This makes the switch very hard to find.

User Behaviour Analytics (UBA): Once someone's username and password is compromised, whoever has them can waltz onto a network and engage in all kinds of

malicious behaviour. That behaviour can trigger a red flag to system defenders if they are employing UBA. The technology uses big data analytics to identify anomalous behaviour by a user.

An 'Attack Chain' comprises of initial penetration, lateral movement and then compromises theft and exfiltration of sensitive data. The middle links in that attack chain have not been very visible to enterprise security pros, and that is why the interest in user behaviour analytics today. Visibility into an activity that does not fit the norm of the legitimate user can close a blind spot in the middle of the attack chain.

Data loss prevention: A key to data loss prevention is 'authentication' and technologies such as encryption and tokenisation. They can protect data down to field and sub-field level which can benefit an enterprise in several ways:

- Cyber attackers cannot monetise data in the event of a successful breach
- Data can be securely moved and used across the extended enterprise, and business processes and analytics can be performed on the data in its protected form, dramatically reducing exposure and risk

High-Performance Computing: High-performance computing (HPC) is essential to a nation's economic competitiveness, scientific discovery and national security. HPC network access has become commonplace as new applications emerge leveraging massive scientific data sets collected by sensors or scientific instruments and new HPC systems support the execution of applications in parallel. This new complexity has heightened HPC security requirements while the existing

pressure to maximise performance remains. New research is needed to determine whether traditional security mechanisms will be effective for next generation HPC systems.

Autonomous Systems: Technologies for autonomous systems and components are maturing and their security implications have been raised often. Research challenges for autonomous systems include manipulation of machine learning algorithms and resulting effects on resilience.

Mobile Devices: Network access usually requires physical connection such as a telephone or Ethernet jack. These constraints have been shattered by the introduction of wireless networking and ubiquitous handheld devices. There are more stakeholders involved in achieving security today, including component and device manufacturers, operating system designers and developers, application developers, cloud storage providers, and network providers. Mobility creates new challenges for protection (e.g., secure update), detection, and situational awareness.

Kill Switch: A kill switch is an event that is used to stop a programme from continuing to execute. A kill switch, also known as an emergency stop (e-stop) and as emergency power off (EPO), is a safety mechanism used to shut off machinery in an emergency when it cannot be shut down in the usual manner.

There also is a debate about implementing kill switches in robots and advanced artificial intelligence systems.

In digital devices, a digitally implemented kill switch is used to protect data by either erasing it, or permanently/temporarily

disabling the device, rendering it unusable by the thief without unlocking credentials from the owner. A kill switch built into the OS of the phone or as third-party app renders devices unusable and ultimately worthless.

French and Israeli electronic warfare units use kill switches to disable opponent military systems. R&D efforts are required to be made in India both for offensive and defensive aspects of the Kill Switch.

Research and Development

Nations and organisations globally are busy developing products, systems and processes for cyber security to safeguard against future threats. There are 11 hard problem areas in cyber security which have been universally identified. These are:

- Scalable trustworthy systems (including system architectures and requisite development methodology)
- Enterprise-level metrics (including measures of overall system trustworthiness)
- System evaluation life cycle (including approaches for sufficient assurance)
- Combatting insider threats
- Combatting malware and botnets
- Global-scale identity management
- Survivability of time-critical systems
- Situational understanding and attack attribution
- Provenance (relating to information, systems, and hardware)
- Privacy-aware security
- Usable security

Cyber security is a complex subject and requires capabilities in a multitude of disciplines. No country will part with its core technologies for cyber security as that would have a direct impact on national security. India needs to develop these technologies as per its operational requirements. The government must bring all stakeholders together with the common aim of developing these technologies as a mission. Technologies recommended to be developed on priority have been listed earlier in this paper. We would now consider the requirements for data security and integrity. The task force recommends the following priorities:

- Extending encryption to allow computation to be performed directly on encrypted data to enable full end-to-end data security
- Quantum-safe cryptography, including implementation-efficient algorithms that are resistant to advances in Quantum Computing should this be necessary
- New data anonymisation methods for enhancing protection of user identity, privacy and confidentiality
- Strengthening the chain of custody of data or transactions using distributed ledger technologies such as blockchain
- Technologies for intrusion, malware and distributed denial of service detection, including new methods for real-time application of network traffic analysis, based on advanced machine learning algorithms
- Malware-based defences to 'live with the threat', analogous to biological defences in living species

- New technologies and models for access control, storage of data, data masking and data erasure
- New resource-constrained crypto and multi-factor authentication technologies for the Internet of Things and other low cost, low energy systems
- New security architectures for hyper-scale cloud infrastructures and highly virtualised computing and communications systems
- Physical layer security for securing communications when cryptography is not possible due to limitations on computational capability, or because of the network architectures involved

The above research topics are being taken up by various governments and agencies globally. In India, research topics have to be chosen carefully keeping in view:

- Short-, medium- and long-term requirements
- Availability of funds
- Requirements of different stakeholders like Ministry of Electronics and Information Technology (MeitY), Ministry of Defence (MoD), intelligence agencies, the Department of Science and Technology, Education Department, Ministry of Home Affairs (MHA), private industry, etc.
- Inter se priority

Contractual Clauses for System Protection and Availability

Supply chain vulnerabilities will remain a major cause of concern for ICT networks and systems of the armed forces till such time

as basic infrastructures for manufacturing of chips and network products are not set up in India. Recent incidents of Meltdown and Specter Malware affected almost all modern processors, including Intel, AMD and ARM chips. Since the initial discovery, variants of both Meltdown and Specter have also been discovered. Similarly, VPN Filter appeared to be particularly interested in targeting networking devices. It targeted devices using default credentials, or those with known exploits. Therefore, vendors need to be bound by contractual obligations to ensure due diligence for protection of networks and data to mitigate vulnerabilities of cross-border supply chain. The vendor also needs to be held accountable for failure of its systems. Contracts may include cyber insurance, and its operability as per the Indian legal system.

Contract Goals

Key contractual goals may include the following:

- Risk identification by analysing and correlating incident logs
- Risk mitigation by ensuring defence in depth and mandated audits
- Risk transfer by effective insurance policies

The vendor must exercise due diligence and set expectations for security (and privacy) right from the RFP stage. It should adhere to Indian Data Protection Law (under finalisation) and respect other provisions of the law of the land. The contract should limit access and processing of data. Curb on remote access by the vendor for maintenance is a security requirement. Disaster recovery and business continuity as part of resilience needs to be ensured through insertions of suitable provisions in the contract.

Vendors that develop a source code for the armed forces need to be bound by the Official Secrets Act. Also, a contract should have provision for the Escrow account. The contract should stipulate that the vendor shall provide secure code training to all authorised personnel and maintain software codes as per the SLP (Software Licensing and Protection) Contract.

Conclusion

India has to develop its own technologies, an electronic manufacturing base, R&D infrastructure and a highly skilled human resource. Being late has an advantage of 'leap ahead', but delays can have catastrophic consequences. There is a need to encourage our industry, provide at least a level field, encourage start-ups and MSMEs and create a vibrant eco-system.

One will have to study and analyse adverse security effects, if any, of the involvement of foreign companies in building our infrastructure. The subject of Cybersecurity and cyber power are complex. The armed forces would need some agency to translate their operational requirement into identifying and exploiting relevant technologies. It is for this reason that the task force has recommended an organisation like WESEE of the Navy, staffed appropriately with Army and Air Force personnel. Further, scientific advisers to the Service Chiefs will have to play a more active part.

India has always responded successfully to challenges to her security. The development of cyber power is a national security objective and a strategic requirement.

India needs to act NOW.

Cyber Power is Offence Dominant and in essence, a sum of intelligence, technology, information sharing, skilled human resource and total synergy. Our culture, actions and policies must reflect these. It is a weapon whose potency increases exponentially when integrated with EW and KE capabilities.

Section Seven

Integration and Development of Concepts for Application of Cyber Power for Effective Cyber Deterrence

Cyberspace is the nervous system of a nation providing connectivity, content and cognition. It is the blending of electronics and electromagnetic energy to create, store, modify, exchange and exploit information. The armed forces see cyberspace from the perspective of Command, Control, Computers, Communications and Intelligence (C4ISR), and connectivity between sensors and shooters. Therefore, the armed forces need a synergy of electronic warfare, cyber warfare and kinetic weapon systems to have force multiplication effect.

In order to understand cyber operations fully at the strategic level, a politico-military framework must be imposed on cyberspace, spelling out the 'Ends', 'Ways' and 'Means' model of strategic analysis, which need to be applied in conjunction with other instruments of coercion and confrontation to achieve a political goal. For cyber operations, ways and means are distinct from other methods because of the nature and challenges in cyberspace. In cyberspace, unlike in the physical battle space, a distinction needs to be made between warlike intentions and criminal/espionage activities to ensure an appropriate response.

Cyber operations are carried out 24/7. In almost all situations, these would precede kinetic operations and would last long after hostilities cease. Under international law, a major cyber incident can be classified as an armed attack. According to the Tallinn Manual, in order to meet this qualification, the cyber operation or tool used must have the same destructive capability or effect as a conventional kinetic operation. This is debatable since today cyber weapons can cause both disruptive and destructive effect.

Further, a disruptive attack could cause immense physical effect too. Political mistrust has converted cyberspace into a theatre of war, and cyber provocations beyond a threshold, even if without due attribution, may lead to both a cyber and kinetic response for which we as a nation should be prepared for. It is only then that we can justify deterrence as our doctrine for the application of cyber power. Article 51 of United Nation Charter provides options for the use of force in self-defence when under a cyberattack.

As of now, cyber power can be applied in support of cyber-enabled operations as an important constituent of national comprehensive power. Pure cyber war is some distance away but is certain and likely to manifest in different shapes and contours as new technologies and threats emerge.

Israel's attack on a alleged nuclear facility of Syria, Russian operations in Ukraine and the recovery of the US drone RQ70 in complete working condition by Iran are some major examples of integrated and cyber-enabled operations.

In 2016, China released its first ever 'National Cyberspace Security Strategy' setting out its positions on cyberspace development and security. Interestingly, the strategy sees cyber security as 'the nation's new territory for sovereignty'. At the 2016 World Internet Conference in Wuzhen, President Xi Jinping declared, 'We should respect the right of individual countries to independently choose their own path of cyberspace development, model of cyberspace regulation and Internet public policies.'

In characterising the Internet as a fundamental domain of state control, China

is challenging long-held assumptions and principles that have governed the Internet and have allowed it to proliferate over the past few decades.

Taking a cue from China, India needs to build all elements of cyber power to ensure national security and sovereignty, and be counted as a leader in the digital domain, taking off from its robust Digital India and Make in India programmes. It should have the ability to defend critical national and military IT infrastructure from cyber-attacks by demonstrated deterrent capabilities – both ‘deterrence by defence and resilience’ as well as ‘deterrence by retaliation’ as given in the recommended doctrine in Section Three.

‘Deterrence by defence and resilience’ would include stated policies and doctrines, organisation and structures, licensing and contractual provisions to ensure accountability of vendors, capacity building regarding R&D, cyber security education and awareness and proactive/active defence leveraging artificial intelligence and machine learning. The resilience of critical infrastructure is required to bounce back in event of an attack.

‘Deterrence by retaliation’ is the ability to conduct synergised offensive operations and the ability to prevent own networks from espionage and interference. Our policies must clearly articulate our position of launching an offensive using both kinetic and cyber power in case the adversary goes beyond the threshold as perceived by us. This position must have complete and declared backing of the political authority.

Finally, it must be understood, both by the policy and decision makers, that cyberspace is an extremely potent domain of strategic

importance and it is imperative that India develop cyber power to support her political aims, ensure her security and sovereignty.

Cyber power is offence dominant and in essence a sum of intelligence, technology, information sharing, skilled human resource and total synergy. Our doctrine, culture, actions and policies must reflect these.

Computer Network Operations (CNO) are increasingly finding acceptance as an attractive, viable, low cost and low technology asymmetric option to undermine sovereignty, target individual leaders and engineer social discord. The ability of the nation-state to survive organised cyberattacks from both state and non-state actors is at the very heart of Computer Network Defence (CND) which will have a decisive impact in preserving sovereignty and social harmony.

The number of intelligent machines on the battlefield is increasing with advancements in Artificial Intelligence (AI) and Robotics. Several such systems like UCAVs and drones are already operational. Many more intelligent weapon systems like drone swarms, combat robots, pilotless aircraft and intelligent space payloads are under active development. Such machines will eventually pervade across conventional battle spaces of land, sea, air and space and lead to a paradigm shift in operational strategy, tactics and organisations. These machines will have autonomous computing capability and will communicate, navigate and synchronise using wireless media and electronic sensors.

Counter-measures and tactics will rely heavily on the use of EW and cyber power in an integrated manner, both for defensive and offensive operations.

Space-based assets play a crucial role in surveillance, intelligence, navigation and communications. While militarisation of space happened almost in the beginning, weaponisation is a recent phenomenon with many nations developing and testing anti-satellite weapons. It is a matter of time before conflicts will be from, to and in space. Integrated cyber and EW capability provides an alternative and potent option for anti-satellite operations.

The Internet of Things (IoT) is another fast developing capability for surveillance and cyberattacks in cognitive, physical and electronic domains. Interference in IoT-based applications of major platforms like aircrafts and ships present a very serious challenge to protect our systems and provide extremely attractive opportunities for offensive tasks.

Synergy, Jointness and Integration

At the tri-services level, air and naval systems have integrated networks, sensors, computer-controlled weapons and navigation systems all of which are typically integrated with platforms (i.e., the aircraft/ship) for the purpose of early warning, survival and stealth. On the other hand, Army's electronic combat assets are mostly platform independent and grouped with field formations as conventional military units.

Aircrafts, drones, helicopters and some classified space assets have highly integrated cyber and EW systems capable of both logical bombing and remote injunction of computer viruses. We will have to closely examine this capability and develop appropriate systems and processes for defence.

Further, there is a definite requirement of integrating capabilities and resources of cyber and Psy Ops, both in planning and execution. Social media in our context is a very powerful dual-use weapon. While we need to quell false news and propaganda, we must integrate all necessary capabilities by way of language, technology, content and so on to effectively conduct 'media warfare.'

Development of Concepts for Application of Cyber Power

Application of cyber power in pursuance of our national aim would require the development of concepts, processes and drills at strategic, operational and tactical levels. This is a big challenge due to the lack of experience, the absence of cyber leaders and inadequate understanding of cyber power as a weapon system capable of disruptive and destructive effects in practically every sphere. It is also a very potent source of intelligence. Cyber power can be applied by itself and in cyber-enabled operations in conjunction with kinetic weapons. Its biggest utility is as a 'Weapon of Information' in cognitive operations and perception management.

Concepts would have to be developed for integrated application in accordance with the Indian Armed Forces doctrine. While training abroad is a must, the learnings must be transformed to Indian requirements. This calls for very innovative, mentally agile and highly skilled human resource.

Each Service must have a cyber range and a network simulation facility for regular training. Cyber operations as part of IW, must form part of every war game, the deductions debated and the conclusions recorded, disseminated and incorporated suitably in battle drills.

Cyber security is contingent on international cooperation in which India should take a leading role. Defence against cyberattacks will only be successful when countries cooperate and mount a coordinated defence. Therefore, nations need to cooperate to de-escalate weaponisation of cyber space, though proactive defence and technological innovation in cyber space are also a necessity. Further, the charter of the United Nations and the existing international legal framework needs to be respected. Nations must talk of cyber peace and not cyber war.

Section Eight

International Engagement and Legal Framework

International Engagement

Challenges for the military in the era of online connectivity and information flows are unique and require a great amount of coordination between nations. They multiply further as cyber space is an integrated civil and military domain and encompasses critical infrastructures, critical Internet resources like root servers, Top Level Domain (TLD) servers, and Country Code Top Level Domain servers (CC-TLD) manned and owned by private players.

The year 2017 was tumultuous for politics, economics, and international relations. The United Kingdom's decision of BREXIT (Britain to exit the European Union), the election of Donald Trump as US President, China's efforts to challenge the world order, the turmoil in Europe over its economy and anti-immigrant policies have all contributed to current geopolitics being vitiated by distrust, which in turn is being reflected in cyber space. The apparent withdrawal of the US from international engagement in cyberspace and China's economic and political advance may well rewrite digital trade rules and openness in ways not envisaged by the Internet's inventors. As part of its efforts to take the lead in the digital arena, China has made it clear that the retreat of Atlantic powers will be complemented by Chinese propositions on digital commons.

Major challenging issues confronting international policy makers are:

- Whether a cyberattack is an act of war and does this mean that it is a use of force under UN Article 2(4)?
- When the nation state is not directly involved, does an act by a single person/group of persons constitute

an act of hostile action on a nation? Whether pulling down a nuclear installation, causing an accident, stealing information critical to national security may qualify for such act? Will this act by individual/group not necessarily confined by geographical borders, automatically imply that the presumed aggressor nation has started the war? And, what should be the response?

- Are attacks on critical infrastructure owned by the private sector that also support humanitarian activities and could be used to achieve military objectives also considered an act of aggression?
- Legitimate cyber worriers are indistinguishable from non-state actors. Therefore, should they be treated as non-combatants?
- How can nations resolve differences in sovereign laws associated with cyber space?
- How do the Geneva and Hague Conventions get correlated in cyber space? Is there a case for a 'Digital Geneva Convention'?

Faced with these challenges, the military across the globe has to effectively defend each nation's sovereignty in cyber space.

Further, nowhere in any domain except cyber space is it easy to remain anonymous. It is very difficult to attribute a hostile act to a nation/individual player. When lethal attacks, such as Distributed Denial of Service (DDoS) attacks are launched, servers from any country can be compromised and a false flag may be raised. Often, the country of origin of

the attack turns out to be the neutral player and the hostile actor is never identified with conviction. Even in the case of DDoS against various countries and the StuxNet attack, the act of warfare in the cyber domain could not be clearly attributed. Attribution to a state is easy but it is more difficult to pinpoint responsibility in case of non-state actors. Thus, the attribution problem marks an important distinction between cyber warfare and traditional warfare regarding intent and identity which are not clearly revealed.

In 2010, 15 countries, including the USA, UK, Russia, China and India advocated an arms control approach to cyber warfare. However, it will take a lot of discussion to define a cyber weapon. And even if that is achieved, major challenges of attribution, dual use of weapons and proxy attacks need to be overcome. Challenges to distinguish between tools for cyber protection and offensive tools prevent control over the proliferation of weapons in cyber space. Control of such tools through the Wassenaar Agreement has not been agreed upon as yet.

Even though, the term cyber warfare has been used for more than two decades, it was only recently that the world saw StuxNet. It employed no fewer than four zero-day vulnerabilities and demonstrated a deep knowledge of the inner working of SCADA. This shows very clearly that weaponising cyber warfare is very complex, involving detailed planning by one or more nation states, non-state actors and private players. A malware specifically affecting only the adversary's network without any collateral damage to civilian/humanitarian networks is still a long way from being productionised on a mass scale and is a great challenge. It is

visualised that weapon stockpiles of the future will include stashes of zero-day vulnerabilities, botnets, control codes and sophisticated malware which cannot be identified openly unlike other weapon systems. Also weapons are not solely controlled by the military/political leadership but most such weapons are mere software residing in obscure covers. How do such weapons deter is a major challenge for international community.

More than 30 states now have commissioners for cyber foreign policy. Denmark has even appointed a cyber diplomacy ambassador. Cyber diplomacy in the widest sense encompasses confidence-building measures (CBMs). It also comprises certain aspects of international norm building, data protection and freedom of expression, Internet governance and prosecution under international agreements for mutual legal assistance.

Many governments, however, have neither the knowledge nor the necessary resources to maintain basic cybersecurity standards, or even ascertain what attacks are being conducted via servers on their territory. Nevertheless, most states voice profound reservations over national sovereignty when presented with the idea of a central global regulatory body for security in cyberspace, thereby rendering it an unrealistic prospect. It is more likely that cyberspace and information space will be increasingly subject to national sovereignty.

On the multilateral level, in 2015 a group of 25 international experts commissioned by the UN General Assembly (UNGGE) reached a consensus that international law should be applied in cyberspace as well, including the right to self-defence. However, in the summer of 2017, the UNGGE could not

agree on whether to establish a so-called attribution council. As a precondition for attribution – meaning the technical, legal and political identification of the perpetrator of a cyberattack – it was decided that sensitive information must be exchanged among Computer Emergency Response Teams (CERTs) and between secret services and security agencies. Ever since multilateral negotiations at the UN level failed in 2017, cybersecurity experts have been calling for ‘coalitions of the willing’ from G20 or G7 states to drive international norm setting forward. Two track formats, such as the Global Commission on the Stability of Cyberspace, predominate.

Strengthening attribution concerns not only states, but also the private sector. In February 2017, Microsoft called for a ‘Digital Geneva Convention’. The most recent initiative, a ‘Charter of Trust’ launched by Siemens at the Munich Security Conference in February 2018, sets the same course. Finally, the World Economic Forum (WEF) aims to create a Global Centre for Cybersecurity to combat cyber-crime and thus, also improve cooperation between the private sector and state authorities, the so called Public-Private Partnership.

These challenges call for international cooperation in which India should take a leading role. Defence against cyberattacks will only be successful when countries cooperate and mount a coordinated defence. Therefore, nations need to cooperate to de-escalate the weaponisation of cyber space, though proactive defence and technological innovation in cyber space is also a necessity. Also, the charter of the United Nations and the existing international legal framework need to be respected. Policy level frameworks must

be evolved to define the threshold and nature of deterrence. Technological innovations need to be adopted to counter non-attributability so that wrong inferences are not drawn. Some of the high profile bilateral, regional and multi-lateral cooperation at international level are as follows:

(a) Bilateral Dialogue on Cyber Issues

- US-China cyber agreement (Sept 2015)
- Both parties agreed not to engage in cyber-enabled economic espionage against each other and refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property
- US-Russia Cooperation on ICT Security (June 2013)
- US-UK Agreement on data access (2016) [Awaiting passage of enabling legislation by US]
- USA-EU Privacy Shield (July 2016)

(b) Regional/international cooperation

- Shanghai Cooperation Organisation (SCO)
Joint proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security was submitted to the UN General Assembly in 2015. India is also incorporated as a Member of SCO since 2017.
- Organisation for Security and Cooperation in Europe (OSCE)
- Adoption of confidence building measures (CBM)

- BRICS and ASEAN Regional Forum
- Regional cooperation on ICT-related security through a number of regional measures including adoption of CBM).
- Expert Group on Cyber Security NATO countries which recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea (NATO Warsaw Summit Communiqué 8-9 July 2016) and collaborative efforts to drive policy issues like publication of the Tallinn Manual Parts 1 and 2.

(c) International Cooperation

(1) World Summit on Informational Society (WSIS)

- WSIS + 10 Review Outcome Document (2015)
- Emphasize on harnessing the potential of ICTs to achieve the 2030 Agenda for Sustainable Development
- Recognise the leading role of governments in cyber security matters relating to national security

(2) United Nations Group of Government Experts (UNGGE)

While the UNGGE of 2013 and 2015 had agreed that international law and the UN Charter apply in cyber space, the 2017 UNGGE reached a stalemate on how international law applies in cyber space and norms and confidence building measures that need to be agreed to by responsible states to avoid cyber conflicts.

(3) London Process

- International conferences on cyberspace to focus on building a new international consensus on its future
- London Cyber Conference (2011)
- Budapest Cyber Conference (2012)
- Seoul Cyber Conference (2013)
- Hague Global Conference on Cyberspace (2015)
- Global Forum on Cyber Expertise
- New Delhi Cyber Conference in 2017

While defence and deterrence are effective in the short term, cyber diplomacy is more promising insofar as contributing to peace and stability in the long run. India needs to take a leadership position by virtue of being the second largest user of cyberspace, in various international initiatives taken at the level of United Nations, ITU, regional bodies and autonomous organisations like Internet Corporation for Assignments of Names and Numbers (ICANN), Internet Engineering Task Force (IETF), etc.)

At present, the coordination of the cyber domain is exercised de-facto by ICANN for its governance, by its control on root servers which are not spread out evenly geographically. Diplomacy is required to exert influence in cyberspace through such organisations and service providers to address large scale attacks. Realising the strategic importance of ICANN, India hosted the annual ICANN Summit in Hyderabad in 2016, where she made a strong case for transparency and democratisation of this international body and urged Indian industry to play a proactive role in its policy making.

Military Diplomacy

The armed forces need to be actively associated with cyber diplomacy because as opposed to overall cyber defence, diplomacy offers the potential for conflict de-escalation and thus for developing norms of state behavior that need to be implemented by the armed forces for peace in cyber space. Further, most conventions/treaties of the pre-ICT era do not cater to situations arising out of cyber incidents/attacks. The international framework should identify such provisions and propose amendments. The orchestration of international accords should be such that norms evolved would limit disruptive activity by states against other states and deter non-state actors.

International engagement is an important aspect of India's cyber security policy. India has cyber engagements with over 15 countries, including the USA, UK, Russia, Japan, Germany, France and member nations of ASEAN. Recently, India signed cyber agreements with the USA, Israel and Russia. CERT-In has also entered into cooperation agreements with its overseas counterpart agencies that are willing to work together and share information in a timely manner. At present 10 such MoUs have been signed.

The task force recommends the following for furtherance of the stated objectives of the Indian Armed Forces Cyber Doctrine:

- India needs to play an active and constructive role in international cyber diplomacy to pursue national security interests
- Cyber diplomacy should be an indispensable component of military dialogue and diplomacy
- Central role of UN in Internet governance and primacy of the state in cyber conflicts needs emphasis
- International consensus on norms of state behaviour need to be pursued in bilateral and multilateral platforms despite failure of the UNGGE 2017
- Military diplomacy should evolve norms and CBMs across the global community with emphasis on arms control in cyberspace

‘Cyber power will flow only through a structured national response towards evolving new strategic weapons in cyber space used by nation states, terrorists or state-sponsored hackers. ‘Defence – surveillance – intelligence – offence’ will go hand-in-hand, backed by appropriate legal empowerment. Without lawful authority, any cyber action on another nation may amount to a cyber-crime for which reasonable laws exist. Additionally, several international engagements are needed to reduce the enormity of scope’.

Legal Framework

Introduction

The world is in the state of strategic transformation as it transcends from industrial age warfare to an information age warfare. Technology is the new normal. It's all pervasive nature, rapid induction and exploitation is accelerating this transformation. Consequently, there is a distinct gap between the technology application and legal framework which may be a decade or more. There is a definite need to reduce this gap and ensure that the procedures, processes and legal framework are made more agile and dynamic. The legal framework, which is generally based on precedence, thus faces an undefined challenge.

The nature of cyber warfare is very similar to naval warfare. All nations having shorelines or owning ships are neighbours. There are no border lines. The area of operation is full of enemies, friends, neutrals and not so neutrals with a fair mix of innocent users of the sea. And like naval forces, cyber forces must abide by a structured legal framework lest they are termed militia/cyber pirates.

For eons, India has had the Chturanga Sena (Quad Services) concept, viz., Thal Sena (Land Forces), Jal Sena (Naval Forces), Nabh Sena (Air and space forces) and Maya (Virtual Power). Therefore, conceptually, cyber war has been an integral part of warfare in Indian scriptures. Cyber war, as warfare in other domains, will be executed within the bounds of the Constitution of India, international laws and treaties where India is a signatory.

Developing norms of states behaviour in cyber space is a challenging task. Cyber weapons such as Stuxnet, DuQu, Flame, WannaCry, Petya, Non-Petya and a long list of

Advanced Persistent Threats (ATPs) are early signs of large-scale cyber war.

The Constitution of India and Cyber War

Any legal framework in India has to emerge from the Constitution of India. Article 352 empowers the President, on the advice of the Council of Ministers, to declare an Emergency in part or whole of India in the case of war or external aggression, or the likelihood of war, or the probability of a foreign attack. The declared Emergency should be approved by Parliament within 30 days. Moreover, the proclamation of an Emergency must be renewed every six months. And, at any stage, if more than 10 percent of parliamentarians write to the Speaker of the House, or to the President of India, Parliament has to re-approve continuation of Emergency within 15 days.

The contours and texture of cyber war is complex and difficult to understand. It is also likely that the government of the day may not like to make all details public to prevent panic as well as not give the opportunity to the enemy to get a battle damage assessment. It will be a challenge for any government to use Article 352 for any pure cyber war situation. Only when cyber war is used in conjunction with physical war, the government may be able to use this provision of the Constitution. It is in the best interest of the nation that Article 352 is not enforced and all appropriate measures, including limited cyber war and cyber defence are initiated without resorting to declaring a state of Emergency. However, there should be a stage where the government may consider a formal response to any cyberattack, with or without the use of Article 352.

On one side it is felt that there is a shortage of quality manpower, while on the other, outside the US and China, we have the highest number of R&D and analytics centres established by the private sector in India. Therefore, probably there is a reasonable amount of quality manpower in IT and IT Security available within India but is sucked-in by the private sector. The shortage is apparently due to exponential growth in cyber-crime, and private industry is not able to cope with it. However, in case of an emergency arising out of a breaking out of cyber war, Article 51A can be invoked to use this manpower for the quick capacity boosting of cyber warriors. Several attempts have been made since 2005 to establish a resource register to facilitate implementation of Article 51A. This project needs revival and more effective implementation. The proposed Cybersecurity Act may make it mandatory to have structured reports and returns for industry and academic institutions.

Cyber Space Jurisdiction

Sections 1(2) and Section 75 of the IT Act, 2000 states that Indian laws related to Information Technology are applicable within and outside India if cause and action fall within the country's territorial jurisdiction. Rule 2 of the Tallinn Manual determines the jurisdiction issue of a state on which the concerned authority can prescribe, enforce and adjudicate all matters, including those that are civil, criminal or administrative in nature. The rule of jurisdiction covers the physical or legal presence of a person (in personam) or object (in rem) on its territory. The manual concedes that there is a difficulty in determining jurisdiction to cloud and grid computing environments. These limitations

are arguments for the physical aspects of information technology as far as jurisdictional issues are concerned. Cyberspace now covers not only physical infrastructure but also data and associated information. With cognitive war becoming an integral part of cyber war, the way information is presented to humans and intelligent machines also become relevant. We may call the presentation of information as content. Therefore, jurisdiction over physical infrastructure, data, information and content is important for exercising the sovereignty of the Indian state.

Rule 2 of Tallinn Manual

Without prejudice to applicable International obligations, a state may exercise its jurisdiction:

- (a) *Over persons engaged in cyber activities on its territory;*
- (b) *Over cyber infrastructure located on its territory; and*
- (c) *Extraterritorially, in accordance with international law*

The Indian cyber-physical territory includes but is not limited to the embassies, high commissions, and consulate satellites and systems owned by the Indian Armed Forces such as aircrafts, ships, submarines, tanks or any other ground vehicles. It is, therefore, recommended that India may exercise and pronounce her cyber jurisdiction as follows:

- Over an entity or a person who is engaged in cyber activity on her territory
- Over the objects related information technology located on her territory

- Over data and content process over her territory
- Extraterritorial, over data or content which is being stored processed or transmitted belonging to the entity or cyber infrastructure within Indian Territory or legal jurisdiction
- Extraterritorial over the entity or a person or a cyber infrastructure or data or content which is the source of or abettor of a devastating cyberattack on any object or person or cyber infrastructure based within the jurisdictional Indian cyber territory
- Extra territorial in accordance with international laws, treaties and agreements

Establish Nation-wide Cyberwar fighting Processes and Procedures

There is a need to establish nation-wide cyber war fighting processes and procedures or what may be called as Cyber War Standard Operating Procedures (CWSOP). Cyber space being ubiquitous in nature requires CWSOP to cover every ministry and department of the Centre as well as state governments. It should also involve industry through confederations and such like institutions.

The CWSOP will form the basis on which cyber war games, drills and exercise can be conducted and measured.

Unless there are reasonably well-defined and written processes and procedures in place, chaos is expected in case of any severe cyberattack. Therefore, there will be a need to undertake various cyber war gaming exercises, starting from paper exercises to

full-fledged all government ministries and departments exercises. The involvement of critical infrastructure, other industries and even citizens should be envisioned and planned.

Reference to the CWSOP can be a guide for control and coordination. It will also create appropriate linkages and introduce responsibility and accountability. Assessment measures and matrices can also be part of it to ensure that everyone undertakes roles with a clear vision of its element in the overall cyber security structure in case of a cyber war or any other serious cyber engagement.

Privacy and Cyberwar

It is likely that cyber operations, on certain specific occasions, intrude into the privacy of an individual. Many countries, including India, are sensitive to the subject and are in the process of framing tougher laws. However, even the Shrikrishna Committee Report as well as the draft Personal Data Protection Act 2018 recommends that the Right to Privacy is a fundamental right in accordance with Article 21 of the Constitution but is not an absolute right, and is subject to reasonable restrictions. These restrictions include national sovereignty, integrity, relations with foreign states.

Article 19(2) of the Constitution states 'Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign

States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence’.

Cyberwar and Deniability

Deniability is a major factor in cyber war. Acts of surveillance, intelligence gathering and non-military intrusion do not amount to an act of war. According to the Tallinn Manual, an operation, even surveillance origination from military base, may be assumed to be an act of cyber war. Therefore, it may be prudent to leave surveillance, intelligence, planting backdoors and dormant cyber weapons to agencies. But its control and coordination should be undertaken through the armed forces in close coordination with the Ministry of Defence.

The orchestration of offensive cyber operations and deception should rest with the defence services even during peace time. Many countries, including US, Israel and China exercise the control over cyber security product companies through a appointed former cyber war expert from the defence forces. Under present law, all listed companies and important unlisted companies should have government proposed independent directors with Cyberwarfare domain knowledge. The government may like to appoint former cyberwar experts as independent directors in all major IT companies and cyber security product companies.

Protection to the Engaging Forces

The tools and techniques of cyber war are similar to cyber-crime – the only differences are the actors, the target and its impact. Therefore, by the very nature of job, cyber war may be termed as cyber-crime, thereby

subjecting their practitioners to legal penal action in courts. At some stage, India will sign the Convention of Cyber-crime (Budapest Convention) or something similar to contain cyber-crime at the international level. It is, therefore, necessary that the government must retain the power to protect cyber forces without giving any explanation to anyone in the public domain. The existing Section 197 of Code of Criminal Procedure 1973, needs to be strengthened.

The Information Technology Act 2000 is focused on empowering cyber commerce and enhancing cyber activities, covering some limited aspects of cyber-crime. It has no mandate to make any rules or regulation for the armed forces and cyber war.

It is, therefore, necessary that a Cyber Security Act is introduced to cover not only various facets of cyber-related crimes, offences, forensics and policing, but also to have enabling provisions for conducting a cyber war and for defence in the event of a similar attack. As discussed earlier, formally announcing a state of emergency using Article 352 may not be practical under most circumstances. Therefore, the Cyber Security Act should empower the Executive to take appropriate action in case of a cyber war, including its precursor and pre-requisite stages. Also, the Cybersecurity Policy, 2013 (which in any case does not cover the aspect of the nation-state at war) has become dated. A faster route to implement initial concepts of cyber war may be included in the new Cyber Security Policy/Strategy. Most countries have empowered themselves through the National Cybersecurity Strategy. The recently released Cyber Security Strategy of the United States of America in its ‘Pillar III: Persevere Peace

through Strength' has elaborated its will to deter a cyberattack and in case of such a situation, impose appropriate consequences on the attacker. Therefore, the Cyber Security Policy/Strategy will form a suitable legal instrument to enhance cyber power.

Amendment to Section 69 of the Information Technology Act

Section 69 of the Information Technology Act empowers government officials to

undertake interception, monitoring and decryption of any information in computer resources. The rules under this section were published on 27th October 2009. These rules do not provide for any situation related to cyber war and defence against cyber war. Therefore, the rules need to be amended to include cyber war forces and the concerned officials should be equally empowered.

Section 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource:

(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-

- (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or*
- (b) intercept, monitor, or decrypt the information, as the case may be; or*
- (c) provide information stored in computer resource.*

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.]

Conventions and Treaties

UN Secretary-General Antonio Guterres has said, “Episodes of cyber warfare between states already exist. What is worse is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it.”

The International community is attempting to create an appropriate convention for cyber war but is failing. The reasons are manifold, including:

- It is at an early stage and nations have not yet developed their full capacity of cyber arsenals, and therefore, do not want any restrictions on it
- There is a lack of consensus on what amounts to a cyber war and how will it differentiate from a cyberattack using (or abusing) non-state actors
- International politics

The ‘Tallinn Manual’ is not even an official document. It is an attempt to map a real-world war in a virtual world, which may not be practical. The ‘Tallinn Manual’ is at the very initial stage of codification of a cyber war but is still years away from practical use. Therefore, the very first step is to segregate acts of cyber-crime from cyber war. To achieve, this ‘Budapest Convention’ is not the best, but a good start point. If an attack is coming from any signatory country, it must first be assumed to be an act of cyber-crime and the signatory country is obliged to protect the victim country from any cyber-crime originating from its jurisdictional area. If no such action is taken, then it can be presumed that the attacking nation-state

has initiated a cyber war or is abetting a cyber war. Therefore, to filter chaff from actual acts of cyber war, the acts of cyber-crime must be identified.

Additionally, India should enter into various bilateral and multilateral treaties to contain cyber-crime. A lesson from China who has taken a step further, is to contain/prevent the precursor stage of cyber war. China has entered into bilateral treaties/agreements with various nations including the US and Canada not to conduct state-sponsored cyberattacks against each other’s private sectors aimed at stealing trade secrets or other confidential business information. Additionally, India could enter into a strategic cyber war partnership with other nations, especially Israel and US to support each other in case of any cyber war on the respective countries.

India with its significant manpower and technical know-how should proactively support weaker nations to establish their cyber defences. It will have a multi-fold impact. Firstly, it will be a formal sign of a reckonable cyber power. Secondly, it will prevent these nations from becoming a source of routed cyberattacks on India. These nations can also become strategic partners in case India comes under a cyber offensive.

The Budapest Convention on Cyber Crime has 57 countries as its members. From the perspective of cyber war it is necessary to filter out cyber-crime from acts of war by a nation state. It will be an arduous task to enter into a bilateral relationship with these 56 countries to ensure that they take appropriate action if a cyber-crime is originating from their country. It is, therefore, necessary that India becomes a signatory to the Convention of Cyber Crime

by the Council of Europe. This will help forces to filter cyber-crime out and can also be used as a ground to formulate lateral discussions on cyber war, as an early agreement at the United Nations is not expected.

Cyber Forensics

Cyber forensics plays a critical role in cyber war to prove any stand in any court of law within India or internationally. To detect intrusion or undertake one, technical analysis may be sufficient, but cyber warriors will be bound by law, therefore, it is necessary that cyber forensics is made part of cyber power forces. There may be occasions when India will have to prove to the international community that a cyberattack has been conducted against India. At that point in time the quality of cyber evidence will be of paramount importance.

It also forms the bedrock of a trust relationship for any bilateral or multilateral obligation. There may be a need to not only technically establish the source of attack emanating from a friendly country, but also may require formal cyber evidence to back that claim.

If the Tallinn Manual becomes the accepted convention of cyber war or is in accordance with the International Human Rights Commission, there exists a definite possibility to prove the many aspects and impact of cyber war on human suffering. Therefore forensic evidence of battle damage assessment may be required to be preserved. Cyber forensics is also necessary for cyber battle damage assessment to recalibrate the next round of attack.

It is, therefore, necessary to have formal cyber forensic experts embedded in cyber forces to meet legal and international obligations.

Rules of Engagement

Presently all efforts of cyber war are fragmented and unstructured at the national level. There is no allocation of areas of responsibility, or distribution of targets. There is no single point of collation of cyber war-related information, let alone control and coordination. This does not mean that various organisations and the three services are doing nothing, but lack of structure has created multiple challenges. Uncoordinated or ad-hoc actions are detrimental to national security. There are unknown gaps, unallocated targets, and over-concentration of surveillance, leading to exposures, fratricide and inflated sense of self-importance. Therefore, a cyber forces coordination centre must be established at the earliest.

Rules of Cyber Engagement (RoCyE) should be defined for the uniformed forces and other cyber forces. To implement RoCyE, there should be a defined state of alertness and readiness. Without having proper defences within the armed forces and across the nation, taking a cyber offensive posture publically could be counter-productive. Therefore, the public stance must be appropriately structured by armed forces, the executive and bureaucracy.

Some Actions/Matters which may be Acceptable as the Rules of Cyber Engagement

- Conjoining with military kinetic action
- Attacks on persons
- Attacks on technical infrastructure
- Attacks on content
- Routing attack through cooperating third party
- Routing attack through non-cooperating third party
- Laws of proportionality
- Laws of proactive defence
- Area of operations
- Choice of cyber weapons
- Protection against fratricide
- Controlling overconcentration and gaps in cyber attack
- Perfidy and ruse
- Surprise, deception and deniability
- Handling of neutrals
- Indiscriminate/unauthorised attack
- Maintaining cyber superiority
- Maintaining cyber dominance
- Cessation of cyber war
- Retraction of cyber mines and booby traps
- Battle damage assessment

(Note: The list is not exhaustive)

Role of Defence Services Headquarters

Headquarters' of Army, Navy, Air Force and Integrated Defence Staff should be involved in cyber war and be directly or indirectly aware of legal provisions related to it. Officers must be made aware of the Information Technology Act 2000 (as amended in 2008), and the changes it has made to the Indian Evidence Act 1886 and the Code of Criminal Procedure 1974. Legal aspects of cyber war should form a part of training curricula and promotion-related examinations. Case studies should be discussed and analysed in various training courses, including the role of the United Nations, ITU and the Internet Governance. At the level of Higher Command and the National Defence College, exercises should include cyber diplomacy and protection of India's interests.

State of Cyber Readiness

Following the State of Readiness, flags are recommended

- Blue – Normal state
- Green – Enhanced Cyber Intelligence/ Surveillance by Nation State/ reckonable non-state actor
- Yellow – Cyberwar likely
- Orange – Cyberwar imminent
- Red – Cyberwar in progress

Preparedness by Defence Forces

All defence personnel, especially of the cyber warfare cadre and Cyber TAs, must be aware of the legal provisions governing their actions. Cyber rules of engagement

must be known to all connected with the cyber command. Training curricula should be amended accordingly. The scope and intensity may vary depending on the expected task to be performed after training. Similarly entrance exams related to promotions and performance enhancement must include questions related to cyber legal matters.

Recommendations and Timelines

Given the aforesaid, following action points are recommended:

- Formally define Indian cyberspace and claim its jurisdiction territorially and extra-territorially (Immediate)
- Take all necessary actions proactively to prevent a situation from reaching a stage of invoking Article 352 (a continuous process)
- Establish a cyber war standard operating procedure for every entity. This will form the basis of measured, nation-wide cyber war gaming, exercises and drills. CWSOP for government ministry and departments should be prepared within a year, the first major cyber war game with two years. By the end of the second year, CWSOP for private entities should be promulgated. A nation-wide cyber war defence exercise should be conducted in the third year
- Amend rules under Section 69 of the Information Technology Act 2000 to empower Cyber forces to undertake interception and decryption (Immediate)
- Introduce a Cybersecurity Act to cover inter alia facets of cyber war (within one year)
- Enter into bilateral, regional and multilateral strategic partnerships for cyber security and cyber war (a continuous diplomatic process)
- Support weaker nations in building their cyber defences (first year onward)
- Sign the Budapest Convention to filter out cyber-crime (Most immediate)
- Enhance cyber forensic capabilities to engage effectively in any international relations for establishing our claims (within one year)
- Establish rules of cyber engagement (within one year)
- Promulgate a State of Cyber Readiness dashboard (Immediate)
- Include cyber legal subjects in training curricula as well as various exams being held by defence forces

Capacity building for cyber deterrence is a national effort and demands involvement of all stakeholders.

Section Nine

Supporting Institutions, Policies and Infrastructure

Cyber security and Cyber power need institutional support primarily due to present and emerging threats. There has been exponential increase, both in the type and intensity of cyber interventions, and extremely rapid advances in technologies. Due to the unique and ubiquitous nature of cyberspace, requisite interventions are required in the international fora, for security and privacy of people. The situation demands continuous action and proactive behaviour. The government cannot do it alone – it is a national effort and demands the involvement of all stakeholders. In addition, institutions and infrastructure are required to support this effort. These are listed below with recommended priority.

Establish National Cybersecurity Commission (NCSC)

The NCSC should be a fully empowered body on the lines of the Space Commission and the Atomic Energy Commission. The commission would be responsible and accountable for cybersecurity across the full spectrum and conduct offensive information operations, including deception, both by itself or integrated with EW and kinetic power. It will formulate and release a national strategy of development and application of cyber power and a National Integrated Cybersecurity Doctrine. The civilian head of cyber security and the military cyber formation commander would report to the Chairman, NCSC.

The NCSC will have the onerous task of creating synergy amongst various stakeholders through an enabling policy and legal framework: developing technology and centres of excellence; skilled manpower with flexible, progressive and innovative

employment rules and facilities; a separate cadre for cyber professionals; crowd sourcing; industry clusters for manufacturing secure products; education curricula; standards and certification; intelligence and counter-intelligence mechanisms; cyber forensics; security standards; cryptography; language experts; and policy research. It will form integrated cyber security teams capable of providing full-spectrum capabilities, conduct periodic audits to ascertain readiness for present and likely threats, and coordinate with all ministries and States for protection of the National Critical Information Infrastructure (NCII) in their jurisdiction.

Cyber Policy Research Centre

There is no think tank or organisation that is studying or analysing policies and documents being produced by governments, industry, civil society, academia, interested enterprise and international policymaking organisations. The thousands of pages that are being churned out require deeper understanding through analysis and discussions to decide what is in India's best interests. We are unable to address policy and operational issues due to the lack of focused studies. Numerous Non-Governmental Organisations (NGOs) created at the behest of foreign governments are obfuscating policy discussions to derail national positions. These attempts have to be dealt with both proactively and aggressively. We are the second largest users of both the Internet and mobile phones in the world and present a very large market. We must ensure that India's voice is not only heard, but also, that no policy detrimental to India is passed. The research facility would make the appropriate expertise available, particularly, when a large volume of cyber security

research and policies requires timely revision as technology evolves.

Integrated Cyber Threat Intelligence Centre

India needs to create a cyber threat intelligence centre which would collect, collate, analyse and share attack data on infrastructure, financial systems, websites and services. It would also correlate 'big data' generated from the government with financial and commercial data to create patterns and identify anomalies for advance preventive actions. It will maintain a comprehensive database on vulnerabilities, kill switches, conduct predictive analysis and be responsible for probing missions.

Indian Cyber security Operations Centre

This will be the nerve centre for conducting information operations across the full spectrum and would be manned by the NCSC. It will work in close cooperation with the Crisis Management Group and have connectivity with all stakeholders.

Assurance Framework, Test and Certification

There is an immediate requirement for setting up a national cyber test facility, providing for network emulation, monitoring and audit, vulnerability analysis, simulated attacks, graduated response, performance analysis and security assurance modelling.

An Agency for Information Security

India is very vulnerable to social engineering, fake news and propaganda that creates the perception of possible governance failure and chaos. Our likely adversaries have and continue to exercise these capabilities on an almost daily basis. There is an urgent need to counter this threat on a real-time basis in view of the tremendous speed of the electronic and social media. India needs an Information Security Agency to proactively counter these threats. This agency would be responsible for the creation of content for our possible offensive.

National Centre for Cybersecurity Resilience

A facility where companies and sector-wide organisations can test security of systems in a contained environment, such as by subjecting a replica electric grid to cyberattack. By applying lessons learned from past incidents, improve the management of future cyber incidents and enhance the country's cyber-resilience, and thereby, raise the level of cyber resilience across the country through a cyber assurance framework and redundancies. For all cyber assets, be it hardware or software, the Centre should have the authority for certification and accreditation of various testing agencies/laboratories across the country to test products as per certification norms

Cyber Command.

In view of present and emerging threats, India needed a Cyber Command (Cyber Formation) yesterday. The announcement of a Defence Cyber Agency is too late and

too little. It indicates a defensive mindset and is contrary to the designed application of technology which is essentially 'Offence Dominant' and the Tri-service Doctrine which talks about deterrence. The government must push this through at the earliest. A delayed decision may land the nation in a serious state of strategic inadequacy. We cannot afford to repeat the mistakes of delayed nuclearisation of India.

National Policies to be Revised and Infrastructure

Capacity building of cyber power for our armed forces is a national imperative and would require enabling policies, total synergy, a clear demarcation of responsibilities between defence forces and civilians, harnessing technology to produce India-specific products and continuous development of skills. Following are recommended:

- Formulate and release National Cyber Doctrine
- Release the Indian Cybersecurity Act at the earliest
- Revise National Electronic Policy-2012 and ensure aggressive implementation
- Revise National Cybersecurity Policy-2013 to include development of full spectrum capabilities for IW
- Develop Standard Operating Procedure for cyber war
- Establish National Academy of Information Security
- Create an Institute of Cybersecurity Professionals anchored on a prominent think tank

- Create a formal Military-Industry Interface for harnessing technology and system development.

While the National Cybersecurity Policy-2013 and the corresponding Cybersecurity architecture deals with the civil aspects fairly in detail, there is a sizable gap when it comes to 'development of cyber deterrence capabilities in the armed forces' and that is precisely the mandate of this Task Force.

Section Ten

Comprehensive Cyber Power at National Level

Cyber power, by its very nature, demands total synergy between policymakers, stakeholders and those responsible for its capability build up and application in the field. Cyber power is a major component of the nation's information warfare architecture. Its integration with EW and kinetic power increases its efficacy manifold and provides different options to commanders for warfighting.

As stated earlier, Cyber space is an integrated domain between civil and military. It must have a single authority responsible and accountable for its protection, security and ensuring safe passage to India for its lawful exploitation.

For the purpose of better understanding, we have theoretically separated the functions of cyber security for civil application, cyber resilience and active defence and cyber power for military applications to include offensive cyber operations and deception.

While the National Cybersecurity Policy-2013 and the corresponding cyber security architecture deal with civil aspects in detail, there is a sizable gap when it comes to development of cyber power in the armed forces and that is precisely the mandate of this Task Force. Recommendations would be incomplete without the methodology for integrating cyber security and cyber power to create 'comprehensive cyber capability' at the national level. Accordingly, this section deals with this aspect with a term of reference of not creating any turbulence.

The Defence Cyber Agency/Cyber Formation has to be integrated with existing national institutions and agencies responsible for various facets of cyber security. We need

enabling policies, processes, transparency, jointness and information exchange to create necessary synergy across the spectrum as mandated in the recommended doctrine.

The armed forces must take part in the decision-making process, and collaborate with major stakeholders to address challenges that continue to hinder timely intelligence and information sharing, joint planning, operations and training, and the development of necessary cyber tools. In this information-dominant era, the armed forces need to have real-time communication with the intelligence community to continuously pursue strategic intelligence to anticipate geostrategic shifts, as well as shorter-term intelligence so that the nation as a whole can respond to the actions and provocations of rivals.

The National Information Board (NIB) is the highest decision-making body for information and cyber operations. It has members from all ministries, security agencies and the armed forces.

The National Security Council Secretariat (NSCS) coordinates and oversees cyber security issues, including Cyber Diplomacy.

The National Cybersecurity Coordinator (NCSC) has been entrusted to coordinate and synergise cyber security efforts.

The National Security Adviser (NSA) chairs the National Intelligence Bureau (NIB) while the NCSC is the secretariat of the NIB.

The IT Act 2000, including its amendment in 2008, provides a comprehensive legal framework to boost e-commerce and also to create an enabling environment for e-Governance in the country. It also addresses

various cyber offences, crimes and protective measures against them.

Operationally, the Indian Computer Emergency Response Team (CERT-In) is the national nodal agency for emergency response and mitigation of cyber incidents, as per the provisions of Section 70B of the Information Technology Act 2000. All organisations have been mandated to report cyber security incidents to the Indian Computer Emergency Response Team expeditiously.

CERT-In is mandated to perform collection, analysis and dissemination of information on cyber incidents; forecast and alerts of cyber security incidents; measures for handling cyber security incidents; coordination of cyber incident response activities; and issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

Armed Forces CERTs are closely collaborating with the National CERT. The Defence Cyber Agency must have real-time communications with CERT-In. Cross-attachments of people from the armed forces and CERT-In is strongly recommended.

The National Critical Information Infrastructure Protection Centre (NCIIPC) is the National Nodal Agency for the protection of critical information infrastructure minus the armed forces and some strategic sectors. However, the DCyA needs to plug into the NCIIPC to enhance protection and resilience of the nation's critical information infrastructure. It must identify the critical defence infrastructure and apply the learnings to ensure their resilience and protection.

National Cyber Coordination Centre (NCCC) provides real-time situational awareness and rapid response to cyber security incidents and enable timely information sharing for proactive, preventive and protective actions by individual entities. Representatives of all stakeholders, including the armed forces, are integrated into the NCCC. Information from the NCCC should be factored into the Threat Intelligence Platform of the DCyA for decision-making. Following are the organisations represented in the NCCC:

- National Security Council Secretariat
- MHA
- MEA
- MeitY/CERT-IN/NIC/STQC
- DOT
- MoD/HQ IDS/Armed Forces
- NTRO/NCIIPC
- DRDO
- Industry/TSP/ISP

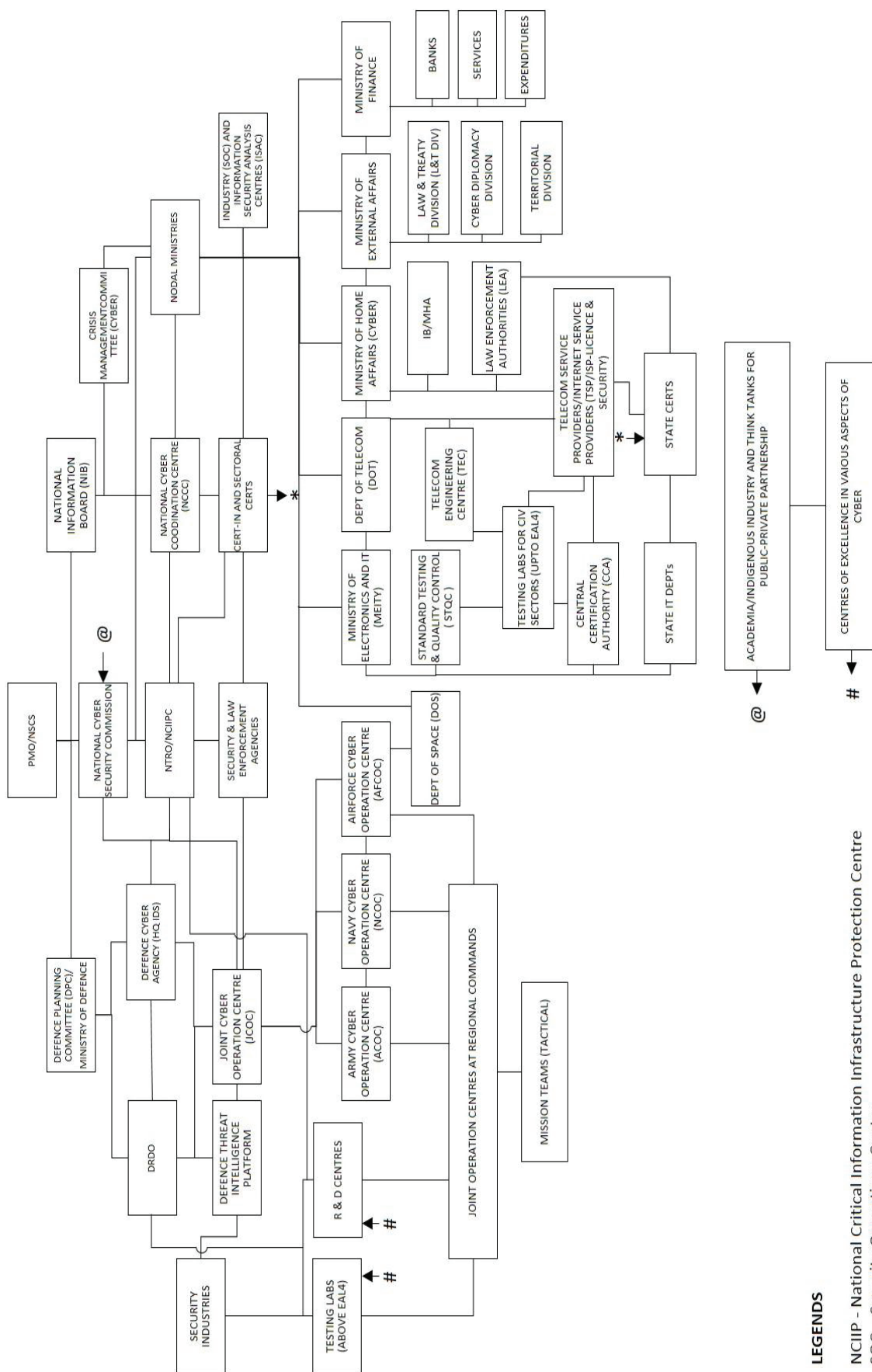
A conceptual schematic diagram of the integration of the DCyA with the appropriate stakeholders is given overleaf.

Recommended Integration of DCyA at National Level

At the highest level, the Defence Planning Committee and National Information Board will give policy directions to the DCyA through the Headquarters Integrated Defence Staff (IDS).

Offensive cyber operations and deception at the national level and special operations will be conducted by the armed forces, duly supported by the DRDO, NTRO and security

Cyber Integration at National Level (Concept)



agencies with input from the Defence Threat Intelligence Platform and the NCCC.

The DRDO and the NTRO will collaborate with industry and R&D establishments to provide offensive and defensive tools. The armed forces will be kept in the loop and project their requirements of cyber weapons and tools for deception.

Cyber resilience of the armed forces networks and systems will be audited periodically and ensured by testing facilities under the DRDO who would also undertake this task for regional commands and integrated mission teams.

The National Cybersecurity Commission, with strategic advisors and domain experts, would control and coordinate the entire cyber eco-system.

Till the formation of the Cybersecurity Commission and the appointment of its head, the National Cybersecurity Coordinator (NCSC) would undertake this task and related responsibilities.

The NCSC will also be the Member Secretary of the NIB (National Information Board), while the CISC would be the Member Secretary of the Defence Planning Committee.

Indigenous industry, academia and think tanks would play a major role for capacity building, public-private partnership for advocacy and expertise by active collaboration and funding from the cybersecurity commission. The armed forces must provide domain specialists to explain their requirements. Most technologies are of dual use.

Several centres of excellence in collaboration with industry and academia would feed into national R&D and testing efforts. The armed forces must interact and have military specific centres of excellence.

The roles of major ministries, including the Ministry of Home Affairs (MHA), the Ministry of External Affairs (MEA) and the Department of Space have been indicated in the Diagram. The MEA has an important role to play in cyber diplomacy, including military diplomacy that could prevent escalation of cyber conflicts.

The Ministry of Finance (MoF) will play a major role not only in protecting national economic infrastructures, but also to enhance the capacity of the DCyA through proper budget allocation.

The task force has recommended capacity building in support of a stated doctrine within a period of 36 months, which encompasses sanction and transformation to a full-fledged Cyber Command and recognition of India as an emerging cyber power.

Section Eleven

Road Map and Action Plan

The road map is illustrated in the summary of recommendations. But any plan is as good as its implementation. With regard to the development of cyber power for our defence forces, two cardinal principles – ‘System Approach’ and ‘Concurrency’ – have to be adopted. Accordingly, an action plan has to be brought into play through simultaneous actions by different entities and that calls for astute project management, delegation of powers and monitoring at the highest level. It is surprising that in spite of a clear pronouncement by the Prime Minister during the Formation Commanders conference in 2014, the development of cyber power in the defence forces has been minimal. This calls for introspection and an aggressive and mission-oriented approach to remove all bottlenecks.

The task force has recommended capacity building in support of the stated doctrine within a period of 36 months which encompasses sanction and transformation to a full-fledged Cyber Command and recognition of India as an emerging cyber power.

The start point would be to issue the necessary sanctioning letters by the government for establishing an appropriate organisation for project management, formation of a steering committee and allocation of funds.

The nominated organisation must have a director for each of the seven pillars. This would be a tri-service organisation under the Headquarters, IDS and would render quarterly progress report to the Chiefs of Staff Committee.

Finally, the task force members would like to place on record their thanks to Dr

Arvind Gupta, Director, VIF, and Lt. Gen. R.K. Sawhney, PVSM, AVSM, Centre Head and Senior Fellow, VIF, and the Staff of VIF for their support and emphasise once again the strategic necessity of urgent capacity building in cyber power within our armed forces and its integration with other components of power. We hope that this report will help the powers that be in decision- making.

Jai Hind

Invited Experts



Dr. Karnika Seth is an internationally renowned cyber law expert and the Chairperson of Lex Cyberia at Seth Associates, the World's first integrated cyberlaws research, forensics and legal consulting centre. Dr. Seth practices law at the Supreme Court of India, Delhi High Court and other legal forums and is the principal legal advisor to many multinational groups and government entities. Her contribution to the growth and development of cyber laws internationally and in India is widely acknowledged in the corporate world and by international organisations, including ICANN and ICMEC. She has been awarded the Digital Empowerment Award (2015) and the National Gaurav Award (2017). She graduated in Masters in Law from Kings College, University of London, and has a doctorate degree in cyber law (Ph.D.) from NIU in 2017.



Air Vice Marshal A.K. Nabh AVSM VM (Veteran). A fighter pilot, he had been working as ACAS Operations (Space), Air Headquarters (Vayu Bhawan) before superannuation in August 2018. The AVM has written many papers and spearheaded a few innovative projects to enhance the combat potential of the Indian Air Force. The Air Vice Marshal was a member of the task force for implementation of Artificial Intelligence in the Defence Services. He has held many crucial Command and Staff Appointments including Chief of Operations, Command of a UN contingent, Director Air Defence Ops, Principal Director (Intelligence), and Principal Director Ops (Information & Electronic Warfare). The Officer, as ACAS Ops (Space), headed and guided Cyber & EW Operations, Media & Publicity Operations, besides Space Operations and Air Traffic Service and airspace management in India.



Jiten Jain, CEO, India Infosec Consortium and Director, Voyager Infosec
Jiten Jain is a leading cyber security expert having specialisation in geopolitical intelligence analysis and mapping them to global cyber conflicts. He is currently heading Indian Infosec Consortium, an independent, not-for-profit organisation of leading ethical hackers and cyber experts in India. He is also the co-founder of Voyager Infosec, a leading cyber security firm specialising in cyber threat intelligence. Jiten is a recipient of the Chevening Fellowship by the British Government and has studied Cyber Defence and Information Assurance at the Defence Academy of United Kingdom. He is also invited by various arms of the Government of India, including its defence forces to train their cyber professionals. He is the youngest speaker to have addressed the Air Commanders

Conferences of Indian Air Force. Acknowledging his authority on cyber security, Amity University has conferred him with an honorary professorship. Jiten is also a visiting faculty at the National Police Academy of India and at the Foreign Service Institute of the Ministry of External Affairs

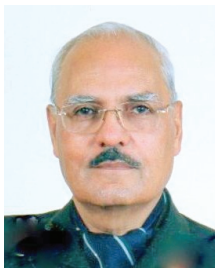


Cherian Samuel. Cherian Samuel is a Research Fellow with the Strategic Technologies Centre at the Institute for Defence Studies and Analyses. He has written on various cyber security issues including critical infrastructure protection, cyber resilience, cyber-crime, and Internet governance. His recent publications include: *Securing Cyberspace: International and Asian Perspectives*, Cherian Samuel and Munish Sharma, eds., Pentagon Press, 2016; 'India's International Cybersecurity Strategy,' in *Cybersecurity: Some Critical Insights and Perspectives*, Damien D. Cheong ed., S. Rajaratnam School of International Studies, Singapore (January 2015); 'Net-Centric Defence Forces: A Macro View,' *DSA Magazine*, July 2014; 'Cybersecurity and National Development,' *CASS Journal*, Vol. 1, No. 3, July–September 2014; 'Cybersecurity and Cyberwar,' *Seminar*, October 2013; 'Prospects for India-US Cybersecurity Cooperation,' *Strategic Analysis*, Volume 31, Issue 2, September 2011. His monograph *Global, Regional and Domestic Dynamics of Cybersecurity* was published in December 2014. He was coordinator of the IDSA Task Force on Cybersecurity, which published a report titled 'India's Cybersecurity Challenges' in March 2012.



Group Captain Ajey Lele (Veteran). Group Captain Ajey Lele (Retired) is a Senior Fellow with the Institute for Defence Studies and Analyses (IDSA), New Delhi. He has obtained a Masters in Physics from Pune University and also a Masters and M.Phil. in Defence and Strategic Studies from Madras University. He has done his doctorate from the School of International Studies, Jawaharlal Nehru University (JNU), New Delhi. His specific areas of research include issues related to Weapons of Mass Destruction (WMD), Space Security, and Strategic Technologies. He has a few publications against his name.

Task Force Team



Lt. Gen. Davinder Kumar, PVSM, VSM Bar, ADC (Veteran). Lt. Gen. Davinder Kumar retired as Signal Officer-in-Chief of the Indian Army in September 2006 after 41 years of distinguished service. He holds three post graduate degrees and five fellowships, and is the only serving officer to get a Fellowship of the National Academy of Engineering. He is a recipient of the Best Engineer award in 2005, a university gold medalist for his Master of Engineering and a gold medalist in B.Tech., having been adjudged the best all round officer. After superannuation, he was the CEO & Managing Director of Tata Advanced Systems Ltd., the Tata Group's lead vehicle in defence, aerospace, and homeland security until September 2011. He has been on the Board of Directors of both public and private sector companies. An expert in electronics, telecommunication networks, information technologies, space technologies, network centric warfare, information warfare and cyber warfare, he was instrumental for the approval and setting up of almost all networks in the army, the Army Cyber Group and the First Information Warfare Brigade of the Indian Army. He headed the national study on Cryptography, was a member of the National Committee on spectrum management and Adviser on IT to the state of Madhya Pradesh. He has worked with the Indian Space Research Organisation (ISRO), Oil India, and the Planning Commission. He was a member of the Hardware and Human Resource Groups of the IT Task Force and the Advisory Committee of National Disaster Management Authority appointed by the Prime Minister. He has over 400 papers to his credit and has been invited to speak at various national and international fora.



Lt. Gen. Anil Kumar Ahuja, PVSM, UYSM, AVSM, SM, VSM & Bar (Veteran). Lt. Gen. Anil Ahuja served in the Indian Army for 39 years and superannuated as Deputy Chief of Integrated Defence Staff (Policy Planning and Force Development) in August 2016. During his military career, he commanded an Operational Corps and a Mountain Division along the Northern borders in Arunachal Pradesh and Assam. He also commanded a Brigade in counter-insurgency operations. He has been India's Defence Attache to Vietnam, Cambodia and Lao PDR (2002–2005) and a UN Military Observer in Angola (1991–1993). Besides extensive operational experience in Northern and Eastern Theatres, he has also held numerous challenging staff appointments. During his tenure as the Deputy Chief, he was the Indian Co-Chair of the US-India Defence Technology and Trade Initiative (DTTI) Inter-Agency Task Force and has been intimately involved with issues of defence cooperation. Besides active military service experience, he has attended professional courses at National Defence College, Army War College and at the Netherlands Defence College. He possesses M.Phil.

degrees in defence and strategic studies. His areas of particular interests include: Northeast India, issues of jointness, higher defence organisation, force development and defence acquisitions. He has served as the Secretary of the Defence Acquisition Council (DAC) for nearly two years. For his distinguished service, he has been awarded PVSM, UYSM, AVSM, SM, VSM & BAR.



Lt. Gen. (Dr.) V.K. Saxena, PVSM, AVSM, VSM (Veteran). Lt. Gen. Saxena has been the former Director General of the Corps of Army Air Defence. Currently he is a Distinguished Fellow at VIF and a Fellow at USI of India. The general is a UN and law scholar, and a prolific writer, having authored five books on subjects like air defence, United Nations, human rights and ballistic missile defence (BMD). He gets published at the rate of two to three articles per month across multiple defence magazines and the VIF. His core competency domains are air defence, aerospace, ballistic missiles, unmanned aerial systems, military communications, cyber security, space, nuclear security, and defence procurement.



Lt. Gen. (Dr.) S.P. Kochhar, AVSM Bar, SM, VSM, ADC (Veteran). Lt. Gen. Kochhar is currently the CEO of Telecom Sector Skill Council of India. He was Signal Officer in Chief of the Indian Army and Principal Advisor for ESDM, Ministry of MSME prior to this. He holds a Ph.D., two M.Phils and an M.Tech. Having a strategic and futuristic vision, he has successfully tenanted positions at corporate board/chief executive/regulatory levels in the government, public sector undertakings, private telecom industry, academic universities and colleges. His area of expertise is the defence industry, skills/academic/ICT/telecom and HR. He is also a speaker at many national and International forums on these and related subjects. He has a flair for finding optimum collaborative-adaptive and inclusive solutions and an ability to implement them quickly and qualitatively. He is known for getting a better ROI for every spend.



Maj. Gen. P.K. Mallick VSM (Veteran). An electronics and telecommunications engineering graduate from B E College, Shibpur, M.Tech. from IIT Kharagpur, and Fellow of the Institute of Electronics and Telecommunication Engineers (IETE), Maj. Gen. P.K. Mallick, VSM is an alumnus of the Defence Services Staff College, Wellington, College of Defence Management, Secunderabad and National Defence College. Commissioned in the Corps of Signals of the Indian Army, the officer has varied experience in command, staff and instructional appointments. The officer has taken part in OP RAKSHAK (Punjab), OP RHINO and OP RAKSHAK in the Valley. He had a tenure of Instructor, Chief Instructor, and OC Junior

Wing in MCTE Mhow. He has commanded a Divisional Signal Regiment in OP VIJAY and OP PARAKRAM in Western Command. A winner of the COAS Gold Medal Essay Competition, the officer is a prolific writer and regularly contributes to defence-related journals and has published more than 50 papers. He has delivered talks and participated in panel discussions at USI, CLAWS, CAPS, NMF, CENJOWS, HQ ANC, Army War College, Military College of Telecommunication Engineering, Mhow, Intelligence School, Pune, Computer Society of India (Bangalore) and Institute of Electronics and Telecommunication Engineers (Lucknow). The Officer was posted as SDS (Army) at NDC, New Delhi, before retirement in April 2015.



Brigadier Abhimanyu Ghosh (Veteran). Brigadier Abhimanyu Ghosh has worked as Officer on Special Duty (Joint Secretary), National Security Council Secretariat (NSCS), handling and coordinating cyber security policy issues. Prior to that, he had a distinguished career of over 35 years in the Indian Army which included stints as UN Military Observer in Angola (Africa), Instructor at Army War College and Chief Signal Officer of a Strike Corps. He steered the nascent Army Cybersecurity Establishment (ACSE) as its Commander for more than three years, with responsibilities as CISO of Indian Army and Head of Army CERT. He holds an M.Phil., M.Sc. (Defence Studies) and a B.E. (Telecommunication). He is a cyber security certified professional holding many certificates, including CISA, CISSP and CEHP. He has represented the Government of India in several bilateral and multilateral international conferences on cybersecurity, including being a member of the Indian delegation at the UNGGE 2013 and 2016. He had the privilege of co-chairing the India-US Cyber Dialogue 2017 and the BRICS Expert Committee Meeting on Information Security 2015. Brigadier Ghosh has written articles on cyber security in various military journals and presented his papers at various national and international platforms.



Brigadier (Dr.) Ashok Kumar Pathak (Veteran). Brigadier Pathak is an Army veteran from the Core of Signals. He held various command and staff appointments, including the UN Mission as an international observer in Angola. He is a certified Black Belt Six Sigma, Ph.D. in Management Information Systems for Warfare: Strategic Implications. He also holds three masters degrees, including an M.B.A., M.Sc. (Defence & Strategic Studies) and M.Sc. (Physics). He is Director at the Maharishi Institute of Management, Noida, Aravali College of Engineering, Faridabad, Army Institute of Management, Greater Noida, and Dean at the School of Business Studies, Sharda University, Greater Noida.



Commander Arun Saigal (Veteran). Commander Arun Saigal is a communications and electronic warfare specialist of the Indian Navy. He held various command and staff appointments, including Commissioning Signal Communication of INS Dunagiri. He is a Fellow of the Institute of Electronics and Telecommunication Engineers and holds an M.Sc. (Defence Studies) from Madras University. Commander Arun Saigal has been an Instructor at the Defence Services Staff College, Wellington, and also at a similar institution in a foreign country. He is an avid reader, researcher and member of many professional bodies. He has been co-opted on the Federation of Indian Chambers of Commerce and Industry (FICCI) Committees on Communications, IT & Cybersecurity. He co-chaired the Cybersecurity Committee for one year. Post premature retirement in 1992, he worked as General Manager (Marketing) with a private company. Presently he runs a company providing consultancy solutions to security and law enforcement agencies.



Commander Mukesh Saini (Veteran). Commander Saini is a veteran naval officer with more than 33 years of experience in Information Warfare and Cybersecurity. A specialist in communication and electronics warfare, he assisted Israel in developing the India-specific EW Payload for UAVs. He was head of National Information Security Coordination cell at National Security Council Secretariat, a precursor to National Information Security Coordinator's office. Most of the information security infrastructures (such as CERT-IN, NTRO, FINCERT) of national importance were created during his tenure. He was also Coordinator of Indo-US Cyber Security Forum. He then joined Microsoft (India) as Chief (Information) Security Advisor. He is founder and MD of XCySS, Cybersecurity Company. He was also Group IT Security head for the Essel Group of Companies. He is an avid writer and speaker on the subject of privacy and cybersecurity. He holds three Masters Degrees and several professional certifications of management, privacy and cybersecurity, including CISSP, GDPR, ISO 27001.



Air Commodore Devesh Vatsa VSM. Air Commodore Devesh Vatsa is an IIT graduate and serving Indian Air Force Officer. He holds a Ph.D. and an M.B.A. Air Commodore Vatsa is a hands-on all communication systems specialist of the Indian Air Force. He has been instrumental in the commissioning of the NOC & DATA Centres of AFNET. He has also been instrumental in implementing various cyber security initiatives in the IAF, including the unified cyber security posture. As AOC, he administers AFNET, IAF Data Centre, NOC/SOC and IAF-CERT. He has been commended by both AOC-in-C and the CAS. For his distinguished services to IAF, he was awarded Vishisht Seva Medal.

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has successfully pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.



Vivekananda International Foundation

3, San Martin Marg, Chanakyapuri, New Delhi - 110021

Phone No: +91-(0)11-24121764, +91-(0)11-24106698

Fax No: +91-(0)11-43115450

E-mail: info@vifindia.org

www.vifindia.org

Follow us on Twitter @VIFINDIA
