CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

INDIAN INFORMATION AND CYBERSPACE: NATIONAL GOVERNANCE ARCHITECTURE AND CREATION OF NATIONAL INFORMATION AND CYBERSPACE MANAGEMENT AUTHORITY (NICMA)

Lt Gen PR Kumar, PVSM, AVSM, VSM (Retd), former Director General of Military Operations. He continues to write and talk on international and regional security and strategic issues.

Introduction. Nation states are in a state of persistent engagement with each other, specially within their regions (except for great powers USA and China who indulge in global intervention to ensure their strategic interests); varying modes of cooperation, competition, confrontation and if national interest is threatened (or even if autocratic leaders feel threatened) even conflict. This multi-lateral and bilateral engagement shave become multi-domain, especially in the realm of warfare and security and is commonly referred to as multi-domain operations (MDO). **Undoubtedly the information and cyber domain has emerged as one of the most critical, pivotal, strategic domains due to its impact on all other domains,** be it PDIME (political, diplomatic, informational, military, economic), or security domains as in kinetic (land, sea, air, space) and non-kinetic (cyber, informational, psychological, legal). It is a strategic necessity that India, a regional power, ensures its interests are protected in the cyber domain, for which governance architecture at the national/apex level cascading down to the lowest (district/corporate/individual) level is created, with a distinct roadmap, constantly updated and revised. The organisation and its personnel need to be robust, dynamic, flexible, professionally trained and manned. Extensive reading and research have been undertaken for this article, and the references (common threads in many articles) from which facts/organisations and thoughts have been gleaned, have been given at

Endnotes[i]. Internationally the UN is making some progress through the 25-member UN "**Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (GGE).**

Cyberspace Sovereignty vis-à-vis Cyberspace as 'Global Commons'. In the traditional physical warfighting domains of land, sea and air, territorial boundaries are, in general, well demarcated. Space, has been declared 'global commons' as per the Outer Space Treaty of 1967, and hence the idea of national sovereignty cannot be extended to this domain. Cyberspace, in contrast, is a virtual domain which lies in the information realm. The Supreme Court of India has ruled that freedom of usage of the Internet is protected under the Constitution. There is an emerging acceptance that there will be better management by replacing *cyberspace* with *info space* as a warfighting domain, covering all the components of Information (IW), Cyber, electronic (EW) and psychological warfare (PSYOPS).

Cyberspace Governance in India: Role and Structure - Salient Aspects

- Defence of our National Cyberspace must be viewed from a national strategic perspective.

- Cyberspace attacks should be considered on the same pedestal as transgressions into our sovereign physical territory. Our national boundaries, whether physical or virtual, deserve to be treated with the same sanctity, and any transgressions of these boundaries should be viewed with the same seriousness and warrant similar responses.

- To bring coherence within the overall national security architecture spanning multiple domains of conflict.

- Role visualized for the MoD/ Armed Forces is in line with their charter vis-à-vis national security in the traditional/ physical territorial battlespace, while that for the MHA [recommend creation of Ministry of Internal Security (MIS) in this paper] corresponds to their traditional role in ensuring internal security and maintaining law and order.

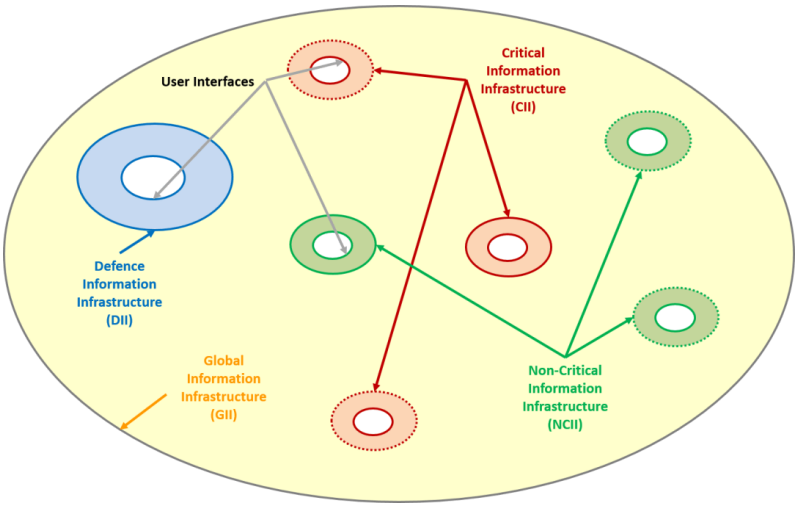
- The role of intelligence agencies such as NTRO is generally restricted to intelligence gathering.

- For any cyber defence strategy to be successful, deterrence and active defence need to be central to the strategy, both of which are based on cyber offensive capabilities being part of our arsenal. The proposed architecture recommends allocating the role of offensive cyber operations to our Armed Forces, in tune with their charter in traditional warfighting domains.

- Armed Forces are well structured to take on the enhanced role envisaged in fifth dimensional warfare, provided a Cyber Command is raised, and the HRD policies are upgraded to nurture much higher levels of specialisation.

- Major step which need to be taken by the PMO/MHA/MIS include the raising of a **new organisation 'National Information and Cyber Space Management Authority (NICMA)'**, and creating fresh training infrastructure for specialist cyber disciplines.

Indian Cyberspace and its sub-structure



Source: Cyberspace Governance in India: Transform or Perish' by Lt Gen RS Panwar, May 19, 2020; https://futurewars.rspanwar.net/cyberspace-governance-in-india-transform-or-perish-part-i/

The Indian cyberspace is the collection of all information systems and intranets (info structure) created by our Nation, including the information which resides within this info structure. Here, "Nation" is not restricted to the State, and includes every national entity, the Indian citizen, as alsoinfo structure outside our territorial boundaries which may be owned by us, which therefore would be included in our National Cyberspace. The National Cyberspace Sub-Structure/National Information Infrastructure (NII) sub-structure could be classified as: -

- **Critical Information Infrastructure (CII**) - broadly identified as networks which fall in the following six categories: Government, Transport, Telecom, Power & Energy, Banking, Financial Services & Insurance, and Strategic & Public Enterprises

- **Defence Information Infrastructure (DII)** - all info structure being owned and used by the Indian Armed Forces.

- **Non-Critical Information Infrastructure (NCII)**

Cyber Structures in other Great Powers

USA

- Integrated and synergised operations by the US Cyber Command, the National Security Agency and the recently established Cybersecurity and Infrastructure Security Agency under Department of Homeland Security.

- The US Cyber Command is tasked with tackling external strategic threatsin cyberspace, while the Department of Homeland Security focuses on cyber threats from the perspective of internal security. US Army is currently carrying out **review and revamping of Organisation and Structures specially related to IW, Information Influence Operations (IIO), and Cyber including functional and basic structure.**

- Interestingly, 13 Cyber Mission Teamsof the US Cyber Command are meant specifically for the protection of CII. Further, the authority for the conduct of offensive operations in cyberspace appears to be vested solely with the DOD.

- **US has already declared that a cyber-attack on its sensitive facilities specially satellites will be construed as an 'act of war'.**

United Kingdom

- Established National Cyber Security Centre (NCSC) in 2016.

- Active defence is central to protection of their national cyberspace.

- For providing cyber operations support at the strategic level, a new National Cyber Force was established in Nov 2020, as a partnership between the Armed Forces and the GCHQ (UK's

intelligence, security and cyber agency), with its primary charter being offensive cyber warfare.

- British Army in 2020, launched 6th Division; organized to focus on cyber, electronic warfare, intelligence, information operations and unconventional warfare.

China

- Is very well structured to defend its National Information Infrastructure (NII).

- The PLA Strategic Support Force has operationalised its well-developed concept of Integrated Network Electronic Warfare as well as the Three Warfare's concept.

- The integration of not only cyber-offensive operations but also of electronic, and psychological warfare capabilities vests with the PLA.

Russia

- Exact details of cyber governance architecture not readily available in the open domain.

- FSB, Russia's domestic security agency and GRU, Russia's military intelligence agency share responsibilities. GRU is known for a culture of "aggression and recklessness" and a "high tolerance for operational risk".

- More recently, SVR, Russia's civilian foreign intelligence service, is increasingly involved in long-term, covert cyberespionage operations.

Outer Space Management. During the 70's, many declared 'Space' as the 4th and final frontier of warfare. Today, however, the virtual dimension of information and cyber, within an electromagnetic spectrum (EMS) is ubiquitous (an umbilical link with space domain at ground, space and satellite levels), and we all are involved in an information and cyber war (competition and confrontation) to safeguard our strategic space in a multi-polar and multi-domain war. Outer space capabilities have become critical to comprehensive national power (CNP) of a Nation.

Increasing importance of Cyber Space Management to the Armed Forces. The US, vide its 'strategy for operating in cyberspace' of 2011 as well as its doctrine on 'cyberspace operation' of 2013, was the first to formally recognise cyberspace as a domain of warfare. The rationale for

the Armed Forces to get involved in the defence of cyberspace; with the heavy dependence on networks in the 21st Century, cyberspace is proving to be of critical importance for the projection of military force, and has been formally designated by many nations in their respective military doctrines as the fifth domain of warfare. India too, in its Joint Services Doctrine 2017, refers to cyberspace as an operational domain. This emergence is arguably the most fundamental change in warfare in the past half century. Networks are emerging as future battlefields, where cyber weapons attack and defend at electronic speeds, using strategies and tactics which are still evolving. Thus, the traditional physical 'battlefield' is gradually metamorphosing into a 'battlespace' with physical, information and cognitive dimensions.

Offensive Cyber Responsibility. One school of thought recommends thatArmed Forces be exclusively tasked with developing and operationalizing national cyber-deterrence/ cyber-attack capabilities. These capabilities would be put to use not only at the national strategic level, but also at military strategic/ operational/ tactical levels across the spectrum of conflict. Full spectrum of strategic cyber conflicts must rest with the Armed Forces/ MoD. Such a charter would cover state-on-state cyber-attacks, which may be restricted to cyberspace alone or be part of a full-blown multi-domain conflict, as also strategic cyber-terrorism and strategic cyber-espionage. Imperative that in India, the Defence Cyber Agency (DCA) be upgraded to a full-fledged Cyber Command. Commensurate transformative changes in HRD and cadre management policies of the three Services. Also, relevant expertise within the DRDO must be placed in support of, and directly accountable tothe Cyber Command for developing suitable cyber weapons and technologies.

Note. While above recommendationswould be ideal and sensible for optimum performance by handing over responsibility to one agency (Armed Forces); but in a multi-domain security environment, where non-kinetic cyber operations are generally strategic and not purely military in nature, handing over responsibility to the Armed Forces in a democracy like India, would require a leap of faith of the policy makers and bureaucrats in India.

Indian Cyberspace Governance: Existing Stakeholders in Government. Those who play a role in securing our NII from a national security perspective.

- **Ministry of Defence (MoD).** Cyberspace as the fifth domain in warfare. Defending assets in domains of space and cyberspace becomes a natural extension of this charter.

- **Ministry of Home Affairs/ Internal Security (MHA/MIS).** Matters pertaining to Internal Security (IS), except in certain special scenarios such as the situation in J&K. Thus, defence against cyber-terrorism and in some cases cyber-hactivism would fall under the preview of the MHA. Cyber-crime though a mandate of the MHA, does not have a direct bearing on national security.

- **Ministry of Electronics and Information Technology (MeitY).** Responsible for the policy, provisioning, monitoring and regulation of IT infrastructurein the country, and hence a significant player involved in the securing of our National Cyberspace.

- **Intelligence Agencies.** Intelligence set-ups within the MoD and MHA, external intelligence agencies such as Research and Analysis Wing (RAW) are also involved in strategic cyber operations as a natural consequence of their mandate.

Current Cybersecurity Establishments.

- **National Critical Information Infrastructure Protection Centre (NCIIPC).** National Nodal Agency for CII Protection. Unit of the National Technical Research Organisation (NTRO), and functions under PMO. Charter includes identification of CII, strategic leadership in cyber threat response, assisting in development of standards and protection strategies, issuing advisories on vulnerabilities and cyber audit, supporting development of relevant cyber technology, organizing training, and coordinating with other cyber agencies including international cooperation. However, protecting the CII lies with the agency running the CII.

- **Indian Computer Emergency Response Team (CERT-In).** Under MeitY with mission of enhancing security of NII through proactive action and collaboration. Headed by the National Cyber Security Coordinator (NCSC); role includes dissemination of information and alerts on cyber incidents, emergency coordination and handling of such incidents, and issuing guidelines and advisories. Broadly speaking, CERT-In looks after the cyber security issues related to the NCII, while NCIIPC focuses on the CII.

- **National Cyber Coordination Centre (NCCC).** A classified project of the Indian Govt, which works as an operational cyber security and e-surveillance agency in India. The first phase of the NCCC, set-up under CERT-In in 2017, handles cyber security intelligence and mitigates online threats.

- **Defence Cyber Agency (DCA).** Limited literature available. Assessed that charter of the DCA restricted to providing cyber operations support to the Indian Armed Forces. The DCA is expected to have a decentralized structure, where the bulk of the Agency will be split into smaller teams embedded within operational forces in the tri-service commands, with the command centre in Delhi.

- **Cyber and Information Security (C&IS) Division, MHA.** Deals with matters relating to cyber security, cyber-crime, and implementation of the National Information Security Policy & Guidelines (NISPG) prepared by it. It has established an Indian Cyber Crime Coordination Centre (I4C) under it to tackle cyber-crime

Optimising of Current Cyber Management Structure: existing gaps

- Current arrangement, under the coordination of the National Security Advisor (NSA) and the National Cyber Security Coordinator, is not able to manage the dynamism of cyberspace. Lack of synergy, working in silos, and palpable lack of direction.

- **An uncoordinated and Defensive Approach: A Severe Limitation.** No Cyber Deterrence Policy. Armed Forces not mandated for Offensive Cyber Operations despite emerging as a pivotal domain of War.

- Response to Cyber Domain as a domain of War needs finetuning.

- The treatment of cyberspace in doctrinal thought and operational planning is far from being at par with the physical domains. As an example, while it is undisputed that in the traditional land, sea and air domains the Armed Forces have the primary mandate to protect every inch of national territory (and not merely defence assets in these domains), in the case of cyberspace the current mind-set is that their role is restricted to protecting only the Defence Cyberspace, and does not cover

the defence of our National Cyberspace. The pragmatic challenge of making armed forces responsible in a democracy has been highlighted earlier.

- **No central cyber fighting force.** Agencies running CIIs and NCIIs are solely responsible for the protection of their respective cyber assets.

- Current strategy is guided more by considerations of tackling cyber-crime and carrying out and countering cyber-espionage. Thus, the imperative of addressing strategic threats in cyberspace, which loom large as part of ongoing multi-domain state-sponsored conflicts, does not seem to have dictated the structuring of the current cyberspace governance set-up.

- Defence Cyberspace being fully air-gapped from the global information infrastructure (GII) considerably reduces its vulnerability to cyber-attacks through the GII, but does not eliminate them, as many mistakenly believe. Also, the strategy of Defence-in-Depth has been operationalized more effectively by the Armed Forces as compared to the CIIs/ NIIs. However, this strategy too needs to be extensively upgraded.

Cyber Defence Strategies

- **Defence-in-Depth.** Presently the Defence Cyberspace is topologically structured as a three-level hierarchy: at the highest level, the entire network is air-gapped from global cyberspace; at the next level there are station access networks, and at the lowest level are networks serving individual establishments. Protection measures are implemented at each level of hierarchy.

- **Cyber Deterrence.** In defence strategies, deterrence precedes protection, resilience, and response. A robust defence-in-depth strategy by itself has deterrence value, referred to as ‘deterrence by denial’.

- **Active Defence.** ‘Deterrence by retaliation’ is quite different from ‘offensive defence’, in that the former implies a “force in being” while the latter involves the actual employment of offensive capabilities. Both need to be incorporated into an effective cyber defence strategy.

- **National Firewall.** National security taking precedence over free flow of information, is almost universally derided by the liberal, democratic world. with the increasing intensity of cyberattacks with significant strategic effects. This view is

gradually undergoing a change, with the notion of 'cyber sovereignty' gaining ground over the current predominant view that cyberspace should remain a 'global commons'. A need to consider setting up of a suitable architecture for firewalling our entire National cyberspace, sometimes referred to as an Internet kill-switch, to be activated in times of national emergencies.

Apex Level Recommendations for better Management of National Security. Currently, the National Security Council Secretariat (NSCS) headed by the National Security Advisor, is the apex body responsible for national security. The National Cyber Security Coordinator, functioning under this Secretariat, coordinates with different agencies at the national level for cyber security matters. It is recommended that the CCS lays down the broad strategic structure and organisation for national security and cyber space management:-

- Set up Ministry of Internal Security similar to Department of Homeland Security; CCS/Group of Ministers (GoM) on National Security lay out the broad framework of organisations and restructuring required for strengthening India's internal security apparatus.

- Set up 'Hybrid and Disruptive Tech Management' organisation to provide road map. Executive branches like AF, CAPF, Intelligence agencies, key ministries and even corporates to build capabilities.

- **Set up 'National Information and Cyber Space Management Authority' in similar lines of National Disaster Management Authority (NDMA).** An overview is provided at the end.

- National Intelligence Grid (NATGRID); an effective National Counter Terrorism Centre (NCTC); synergised Multi Agency Centre (MAC) and finally, linking all these agencies on secure data links.

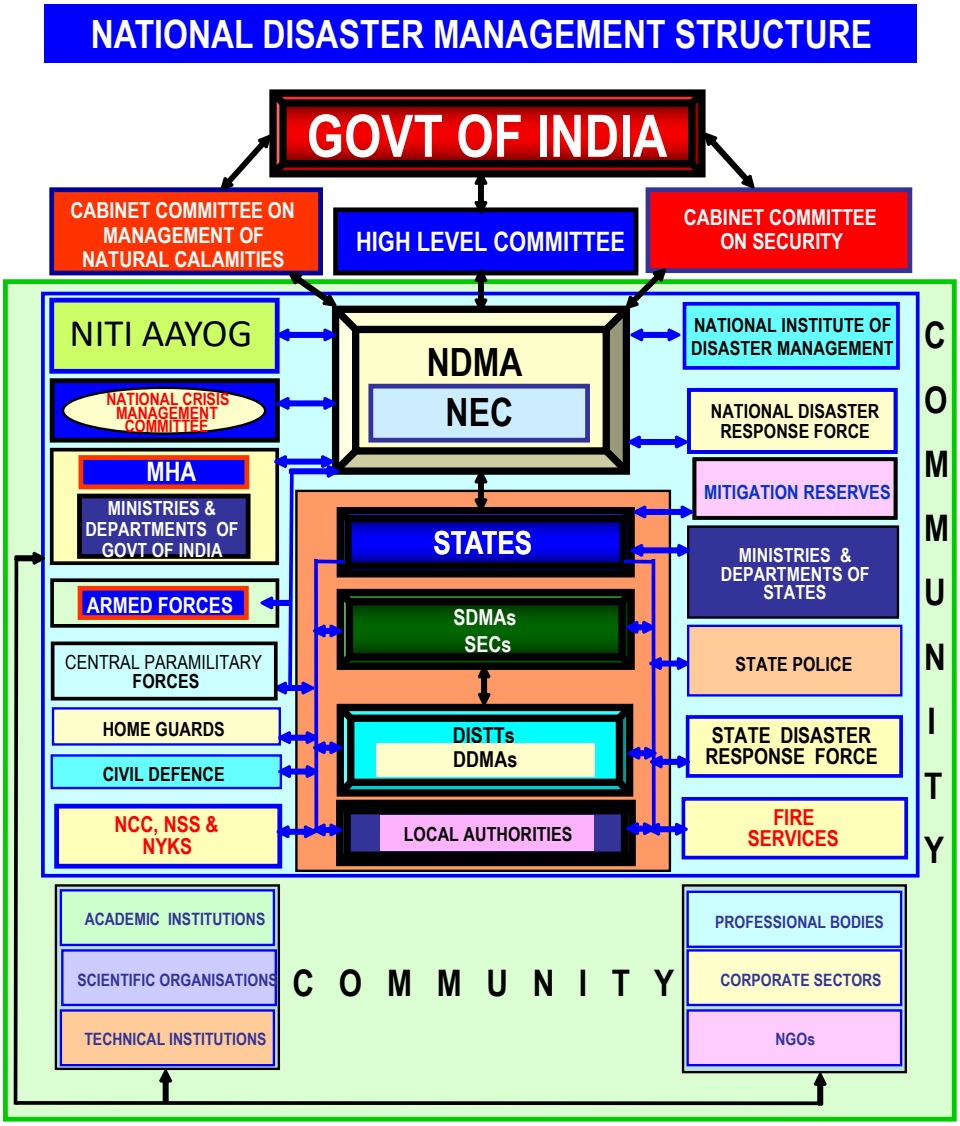
- Enhancing security consciousness of the average citizen.

- **Matrix based Organisations and Functions**.Strong vertical and 'cross- cultural' institutionalised linkages at apex political, diplomatic and military levels; encompassing administration, law enforcement and intelligence agencies at the national, state and district levels.

- **Vertical and Horizontal Interface of Security Actors. Holistic,** with NDMA, science and technology and infrastructure development organisations in public and private sectors (to include hygiene, water and sanitation), health industry, customs and immigration, commerce, aviation, shipping, railways and tourism, schools, colleges and educational institutions, the media (especially social media) and many others; Information and intelligence would have to be shared seamlessly.

A New Approach to Info and Cyber space Management: Create 'National Information and Cyber Space Management Authority (NICMA)'

NDMA. The organizational structure is placed below:-



-INTERACTIVE NOT HEIRARCHIAL

-VERTICAL AND HORIZONTAL LINKS-THREE TIER SYSTEM

-COMMUNITY PARTICIPATION ESSENTIAL

Overview of NDMA

The NDMA Act was enacted in parliament by the Government on June 2005, and the National Disaster Management Policy was promulgated on 26 Dec 2009, thus providing it apex executive authority, oversee, financial flexibility and most importantly central and state support. The PM is the Chairman of NDMA. Its structural and organizational characteristics are:-

- Paradigm shift from response centric to a holistic and integrated approach. The focus has also shifted to a community awareness approach participation approach.

- Backed by – institutional framework and legal authority.

- Supported by financial mechanism, creation of new funds i.e. response fund and mitigation fund.

- Disaster Management (DM) structure – at all three levels i.e. national, state (CMs as chairpersons) and district (DMs as chairpersons and chairman of Zila Parishads as co-chairpersons).

- National and state executive committees (NEC/SEC) to assist these authorities at different levels functioning effectively. The NEC is chaired by the Cabinet Secretary while the SEC is chaired by the Chief Secretary.

- NDRF (National Disaster Response Force) created. A substantial, well equipped, trained, experienced and enthusiastic force which is building strong ethos and DM culture similar to the Armed Forces. Similar State response forces are set up. They have specific disaster centric SOPs and equipment packages positioned at disaster prone areas.

- NDMI (National Institute of Disaster Management) which is the mother node training centre for establishing policies, SOPs and to ‘train the trainers’ set up.

- As can be seen from the structure, other mainstream agencies involved in every facet of DM management are equally involved top down and parallelly from Ministries and departments from Central and State governments, Armed Forces, Paramilitary and Police forces, Home Guards, Civil

Defence setups, local authorities, even corporates and the youth through NCC and NSS (National Service Scheme).

- It is the constitutional obligation of the Armed Forces to come to the aid of civil authorities not only for internal security, law and order but DM situations. Armed Forces form part of organisation at each level [the Chief of Integrated Staff (CISC), and DGMOs of tri-services form part of the NEC], being deployed all over India and with the training and culture for DM. Traditionally, they have been first responders but both by designation and deployment the NDRF battalions are now the first responders, are getting better with specific training and equipment to deal with a particular disaster.

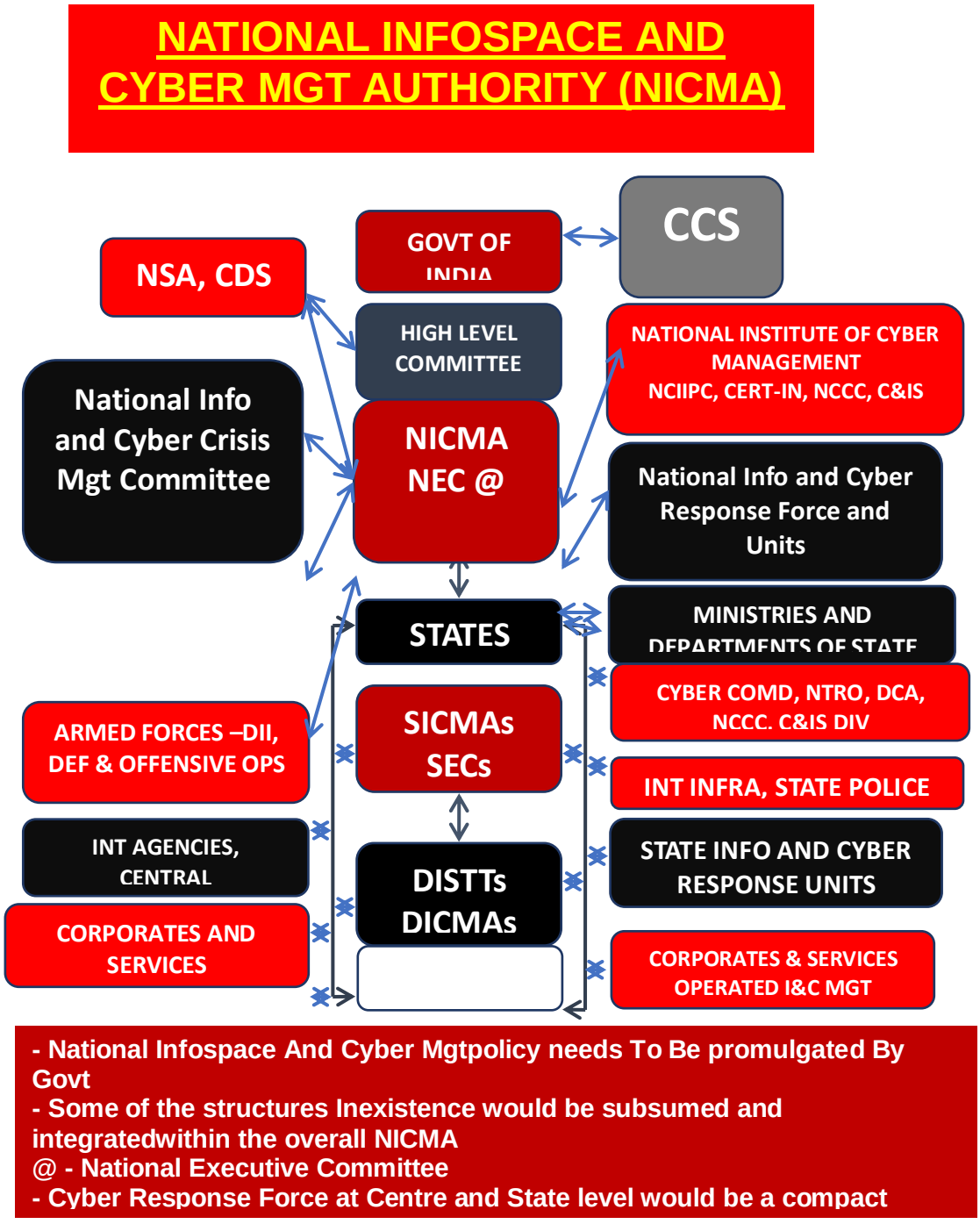
- Rehabilitation, mitigation and 'build back better' is as important an activity as DM and relief, for which finances and resources are catered for.

- The NDMA with its NDRF has now got universal acceptance and conducted international DM both pro-actively and reactively based on request of other foreign governments.

Formation of National Information and Cyber Space Authority. An organisation structure is presented below

National Vision. To transform Indian information and cyber space into a seamless National grid, which will be holistically, effectively, synergistically managed in a time-sensitive and integrated manner.

The organizational structure could emulate the NDMA.



The NDMA is a fully operational setup, which has come out with flying colours conducting multi-faceted complex DM operations from the national to the local level whenever called out. One has read numerous papers and articles on the pivotal role and value of Information and Cyber operations in multi-domain operations/warfare, which mainly resonated with the view that there is no singular, integrated, synergised national set up to manage the fifth domain which operates 24X7 impacting all other domains, and all agencies/committees/institutions working in their respective silos. Unlike other domains, due to its vast scope, totally different characteristics of being cognitive/non-kinetic with no specific limitations; managing

synergistically from the tactical to strategic/national level is a big challenge.

After studying the organisation, functioning and effectiveness of NDMA, one has reached a conclusion, that with some modifications (naturally) creation of a similar organisation would ideally suit info-cyber space management. The cyber defence strategies of defence in depth, deterrence, active defence and activating a national firewall can be best laid out and executed by NICMA.The broad organisational structure has been illustrated above. Except for cybercrime (here too, cases which have national security implications or which are sensational/sensitive/national in nature can be handed over to NICMA, just like law and order cases are handed over to NIA/CBI/IB/ED by the state police), the other dimensions of Cyber-attacks listed below (executed by internal forces or/and by foreign inimical nations/agencies) can be optimally protected, and in turn pro-active operations can be undertaken by NICMA.

- Cyber Hactivism – by cyber activists for pleasure, philosophical, political or non-monetary reasons.

- Cyber Espionage – by cyber spies to steal govt and non govt proprietary info to gain strat, security, financial or political gains.

- Cyber Terrorism – state andnon-state actors.

- Cyber War – all types of attacks by cyber warriors again state or non-state actors.

- Monitoring information and cyber space for inimical and sensitive inputs which impact/ could impact national security and taking defensive and offensive actions.

- **Offensive and Punitive cyber operations (responsibility given to one agency, preferably the Armed Forces in consultation with NSA/NSCS).**

Conclusion. Information and Cyber space domain have undoubtedly emerged as a pivotal and maybe even existential domain to be pro-actively managed, from the national security and growth perspective. Abroad overview of the proposed organisational structure NICMA, has been attempted. Some of the structures like NCIIPC, CERT-IN, NCCC, C&IS would need to be reviewed and merged for better optimisation. The shortage of trained professionals for this extremely dynamic, vast and

complex domain will pose a challenge. However, given India's proven record in IT, it is not unsurmountable and is an essential ingredient to manage the domain. This cohesive structure which brings all the existing elementsunder one umbrella, with an apex authority at the highest policy making level, guaranteed funding and monitoring, would catalyse and synergise national information and cyber space operations, and most importantly be able to tackle future challenges.

CERTIFICATE

The paper is author's individual scholastic articulation. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS.

Author has been reading large number of articles, professional journals on the subject. There is a fair amount of overlap. No specific part has been directly referenced, but facts and thoughts have been paraphrased, since many aspects are factual like the existing organisation structures for cyber and space management. **The proposed structure of NICMA is an original recommendation.**

[i]- Author is grateful for three-part article of Lt Gen RS Panwar (Retd) titled "Cyberspace Governance in India: Perform or Perish" which has been used extensively in this article. Available at https://futurewars.rspanwar.net/cyberspace-governance-in-india-transform-or-perish-part-i/. Accessed from 01 Sep to 06 Sep 22.

- Articles by Lt Gen PR Kumar (Retd) titled "Organisation and Structures for IW and Influence Operations In Indian Context" (https://cenjows.in/pdf-view/?url=2022/03/Synergy_Aug_2019_BW.pdf&pID=11494); "Information and Psychological Operations: Emerging Force Multipliers" (CLAWS journal 2020); and "Space and Cyber Warfare: An Umbilical Bond" (https://www.claws.in/publication/space-and-cyber-warfare-an-umbilical-bond/?fbclid=IwAR2QHWl0OIBvYf7s06MaW7MbTlVz38oRyXOCMOibtDh8joijKYwYtJ_QEiM) published by Centre for Joint Warfare Studies (CENJOWS) and Centre for Land Warfare (CLAWS).

- "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance", by SerkenSavas and Suleman Karatas, published 11 Jan 2022, https://link.springer.com/article/10.1365/s43439-021-00045-4. Accessed on 20 Aug 22.

- From Google Search; using tag 'national cyber governance structures of different nations'

- NDMA, GoI site available at https://ndma.gov.in, and https://nidm.gov.in

- "ORGANISATIONAL GOVERNANCE OF CYBERSPACE IN INDIA" by E Dilipraj and Ramnath Raghunadhan, AIR POWER Journal Vol. 13 No. 1, SPRING 2018 (January-March) from CAWS (College of Air Warfare Studies), available at https://www.researchgate.net/publication/332402995_ORGANISATIONAL_GOVERNANCE_OF_CYBERSPACE_IN_INDIA.

- SaikatDatta, "Defending India's Critical Information Infrastructure: A report", 2016, available online at https://internetdemocracy.in/reports/india-nciipc-saikat-datta-2016/; and "Defending India's Critical Information Infrastructure: A report", 2016, available online at https://internetdemocracy.in/reports/india-nciipc-saikat-datta-2016/. Accessed on 02 and 03 Sep 22 May 14, 2017.

- IDSA Task Force Report March 2012, INDIA'S CYBER SECURITY CHALLENGE, Institute for Defence Studies and Analyses, New Delhi. Accessed on 31 Aug 22.
- "India's tryst with a New National Cyber Security Policy: Here's what we need", 04 Aug 21, Financial Express, available at https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053/. Accessed on 04 Sep 22.