# 8. Cyber and Space Strategy for India

Major General P K Mallick, VSM (Retd)

**Introduction**

The emergence and evolution of cyber space have been an enormously positive force, contributing to globalisation, the creation of a new global commons, the rapid spread of knowledge and ideas, the development of global markets for local products and the empowerment of individuals and small groups. Yet, cyber space also facilitates intensified government surveillance of its citizens, creates new opportunities for criminality, provides new avenues for terrorist recruitment and adds a new playing field within which geopolitical rivalry among great and not-so-great powers plays itself out. The remarkable growth of digital data, continued increases in bandwidth storage capacity and improvement of raw computing power have all had a profound impact on societies. The cyber domain connects a vast array of people, ideas, computers and machines through the information environment. Because the cyber domain intersects throughout the land, maritime, air and space domains, cyber action is itself an integral part of military operations in all domains. Governance mechanisms lag far behind the continuing exponential explosion of technology innovation in cyber space.

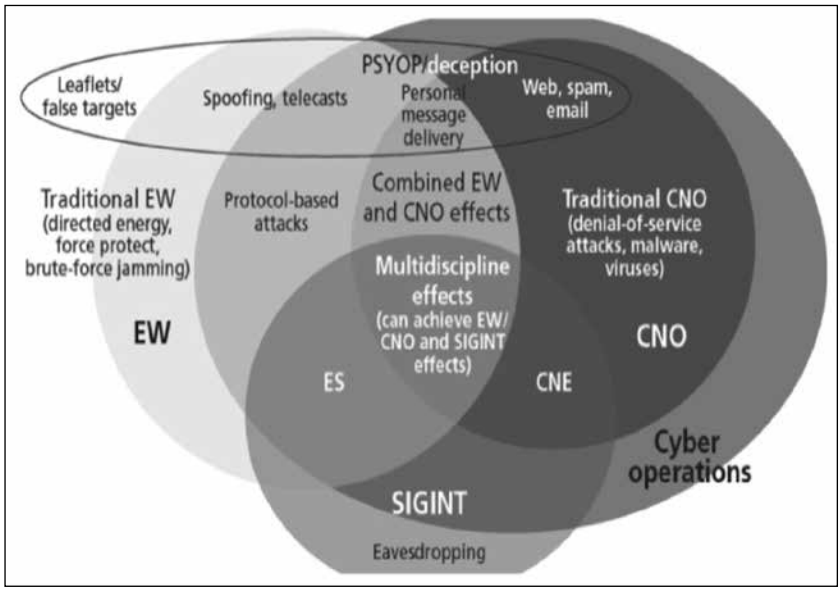
The relationship between the space and cyber space domains is unique. Space operations depend on the Electro-Magnetic Spectrum (EMS) for the transport of information and the control of space assets. Many cyber space operations occur in, and through, the space domain via the EMS, resulting in an interdependent relationship between space and cyber space.

In today's age of specialisation, convergence of domains is taking place. Recently, the US Army has put all the Centres of Excellence (CoE) of Cyber Warfare, Electronic Warfare (EW) and Signals Intelligence (SIGINT) in one place. The integration and synchronisation of Cyber Electro-Magnetic Activities (CEMA) is a new concept. In 2014, the US Army came out with its first doctrinal Field Manual (FM 3-38) on CEMA. Cyber electro-magnetic activities are activities leveraged to seize, retain and exploit an advantage over adversaries and enemies in both cyber space and the electro-magnetic

spectrum, while simultaneously denying and degrading adversary and enemy use of the same, and protecting the mission command system. CEMA consist of Cyber space Operations (CO), Electronic Warfare (EW) and Spectrum Management Operations (SMO).

In April 2017, the US Army published its Field Manual (FM 3-12) on cyber space and EW operations. The electro-magnetic domain is explained in the following diagram[1] (Fig 1).

**Fig 1: Electro-Magnetic Domain**




The ability of the armed forces to exploit cyber space and EW capabilities will prove critical to the success of any military operation. As cyber space and EW operations develop similar and complementary capabilities, the armed forces must plan, integrate and synchronise these operations with their plan of operations.

In Operation Orchard, Israel used cyber tools to support combat operations, such as the air strike on a Syrian nuclear reactor in 2007. In this incident, the Israeli Air Force was able to fly into Syrian air space and bomb the reactor without alerting Syrian air defences. To accomplish this, Israel reportedly took control of the Syrian radar systems and tricked them into thinking that nothing was happening, even while the attack was underway. Israel chose not to blind

the Syrian defences, or shut them down, which would have alerted Syria to trouble, but instead temporarily reprogrammed the systems to make it appear that they were functioning normally. This was the first demonstrated example of use of cyber warfare and electronic warfare tools together.

**Relation Between Cyber Space and Space**

Space and cyber space are increasingly interdependent. Much of the world's critical infrastructure such as communications, transport (land, maritime and air), energy (conventional, renewable and nuclear), financial transactions, agriculture, food and other resources management, environmental and weather monitoring and defence depend on the space infrastructure, including satellites, ground stations and data links at the national, regional and international levels.

Satellites and other space assets are vulnerable to cyber attacks. New vulnerabilities and threats to space assets are created by the increased link between space and cyber space. The sheer scale of data gathered, processed and transmitted by satellites on a daily basis offers great vulnerabilities to be exploited by a cyber attack. Space and cyber capabilities ride on the same infrastructure. The bit of data may ride on fibre for a while before being directed up through a satellite and back down to another terrestrial network. Space and cyber space capabilities are distributed, networked and global. Each of these depends on the electro-magnetic spectrum and Information Technology (IT) infrastructure that affords great capabilities but also creates cross-domain vulnerabilities and challenges.

The risks associated with cyber attacks are : taking physical control of satellites, such as manoeuvring a satellite so that it collides with another satellite, 'decaying' or lowering its orbit so that it reenters the Earth's atmosphere and burns up or deliberately overexposing a satellite's solar panels to highly energetic ionising solar radiation, causing irreparable damage.

Cyber attacks on satellites can include jamming, spoofing and hacking attacks on communication networks; targeting control systems or mission packages; and attacks on the ground infrastructure such as satellite control centres. Possible cyber threats against space-based systems include:

- State-to-state and military actions.
- Well resourced organised criminal elements seeking financial gain.
- Terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions.
- Individual hackers who want to publicise their skills.

The likely consequences of cyber attacks on space infrastructure could be :

- Reduction in national security or defence capability.
- Reduction in capacity of communications, observation capability or navigation precision.
- Corruption of communications, including precise timing systems, leading to lack of confidence.
- Denial of orbits following a contrived collision.
- Destruction of a space vehicle, or holding it to ransom.
- Destruction of a complete launcher and payload assembly, possibly during the launch phase, putting the uninvolved general public at risk.
- Corruption or deletion of data being transmitted from satellites.
- Interception of communications including sensitive intellectual property.
- Rerouting of communications to allow easier interception.
- Jamming of signals or spoofing of data.

Development of a flexible, multilateral space and cyber security regime is urgently required. One may safely argue for a combined space and cyber space common where the constant stream of technological and commercial developments allows for a seamless integration of internet-based capabilities into space systems.

## Cyber Strategy

### *Introduction*

Cyber space can be defined as: "A global domain, within the information environment, whose distinctive and unique character is framed by the use of electronics and electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communication technologies".

The US Department of Defence (DoD) defines cyber security as the prevention of damage to, protection of, and restoration of, computers, electronic communications systems and services, wire communications and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.[2]

Cyber elements include all digital automation, including those used by the defence Services and their industrial base. This includes Information Technology (IT) embedded in weapon systems and their platforms; Command, Control, and

Communications (C3) systems; Intelligence, Surveillance, and Reconnaissance (ISR) systems; logistics and human resource systems; and mobile as well as fixed infrastructure systems. "Cyber" applies to, but is not limited to, "IT" and the "backbone network," and it includes any software or applications resident in, or operating within, any defence systems environment, which is commonly collectively referred to as Information and Communication Technology (ICT).[3]

Cyber space is a man-made domain unlike land, see, air and space. There is a school of thought that cyber space as a domain of warfare, is neither a definitive nor insignificant domain – it will neither win wars alone or be utterly useless during conflict. Cyber space is a more complex strategic domain than the other four strategic domains (air, land, sea, and space). It demands more complex response calculations. This provides significant difficulty for strategic planners and decision-makers who seek to accurately identify the true locus of the threat, attribution of the perpetrator, time available to respond, and response options. Government decision-makers have to be flexible and adaptable, and approach solutions with open minds within an agreed upon strategic framework.

The current balance of cyber power favours the attacker. This stands in contrast to our historical understanding of warfare, in which the defender has traditionally enjoyed a home field advantage. In practice, the cyber components of most armed forces devote most of their capabilities to protecting military networks, though a growing number of states have declared a capability and intent to undertake offensive cyber operations. The role of the armed forces in securing national networks is far from clear, as is their capacity to contribute to achieving it.

**Cyber as Part of National Power**

Cyber space shares the characteristics of both a dimension and an instrument of national power. As a dimension of national power, a nation can leverage cyber space as it does any other strategic dimension, using it to persuade, entice, coerce, deter or compel an entity to act in a certain fashion. As an instrument of national power, cyber space includes key components such as interdependent networks of information technology infrastructures and resident data, including the:

- Internet.
- Telecommunications networks.
- Computer systems, especially software.
- Embedded processors and controllers.

We need to be clear about the following for any action in cyber space :

- **Authority:** Who acts, where, and when?
- **Response:** What actions to take? What are the rules of engagement?
- **Impact:** What are the likely consequences of a response?
- **Resources:** What are the scope and scale of the following actions:
  - Which dimension(s) of national power to use and in what mix?
  - Which domain(s) to act within?

The overwhelming majority of military uses of the cyber domain have been aimed at securing shortlived tactical advantage on the battlefield. But at a strategic level, governments are struggling to work out how to combine the capabilities of their armed forces with other instruments of national power to create the kind of 'all-of-nation' capabilities and responses that a new set of challenges appears to demand.[4]

Nation states have documented their cyber strategies and executed them in the form of Cyber Commands. The military dimension has seen cyber space witnessing the beginnings of a race for the development and deployment of cyber weapons. Non-state actors, such as terrorist organisations and criminal syndicates, have become tech savvy, employing human resources to develop malware. These tools are used extensively in committing cyber crime. Terrorist organisations leverage the benefits of cyber space, harnessing it for ideology propagation, recruitment and communication.

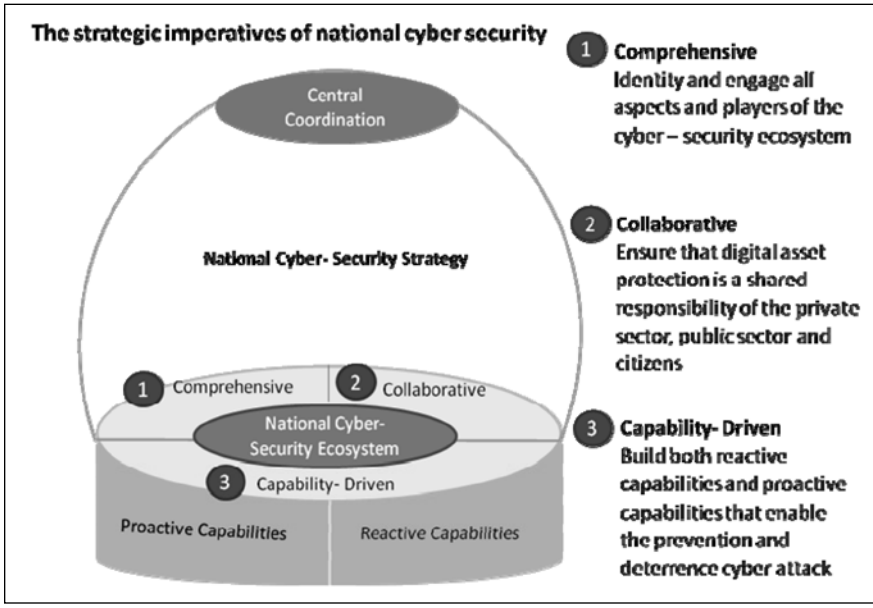
Cyber security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organisational behaviour, political science, engineering, sociology, decision sciences, international relations and law. Although technical measures are an important element, cyber security is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details.

A substantial part of the strategy document should remain open to the public. Such a document should also include sections for classified issues that should remain undisclosed and that will assist in coordination and synchronisation of the defence organisations operating, as far as this is possible. Formulating the document is an important and achievable challenge.

**National Cyber Security Strategy-Making Process**

The strategic imperatives of national cyber security may be explained by the following diagram (Fig 2).

**Fig 2: The Strategic Imperatives of National Cyber Security**




The process of making a national cyber security strategy is explained in the following diagram (Fig 3).

**Fig 3: The Process of Making a National Cyber Security Strategy**

**What is a National Strategy for Cyber Security?**

The IT giant Microsoft Corporation has published a remarkable document called *National Strategy for Cyber Security*.[5] It states that a national cyber security strategy outlines a vision and articulates priorities, principles and approaches to understanding and managing risks at the national level. Priorities for national cyber security strategies will vary by country. The most successful national strategies share three important characteristics.

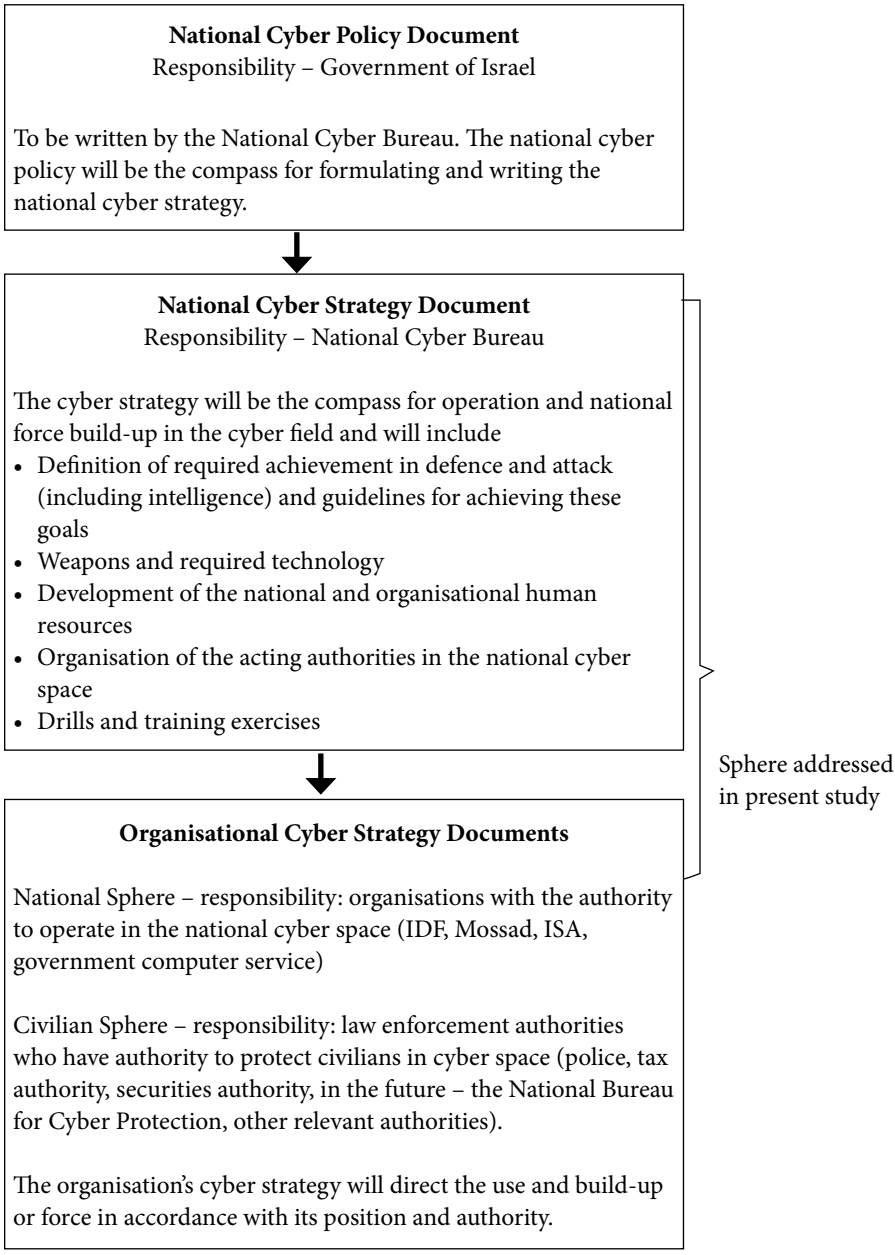
- They are embedded in "living" documents that have been developed and implemented in partnership with key public and private stakeholders.
- They are based on clearly articulated principles that reflect societal values, traditions and legal principles. Programmes created by the government in the name of security can potentially infringe on these rights and values if not articulated and integrated as guiding principles.
- The strategies are based on a risk-management approach where governments and private sector partners agree on the risks that must be managed or mitigated, and even those that must be accepted. A national strategy, if developed correctly, can meet many needs of the government, the private sector and the citizens of the country.

Microsoft recommends the following six foundational principles as the basis for a national strategy:

- **Risk-Based:** Assess risk by identifying threats, vulnerabilities, and consequences, then manage it through mitigation, control, cost, and similar measures.
- **Outcome Focussed:** Focus on the desired end state, rather than prescribing the means to achieve it, and measure progress towards that end state.
- **Prioritised:** Adopt a graduated approach to criticality, recognising that disruption or failure are not equal among critical assets or across critical sectors.
- **Practicable:** Optimise for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors.
- **Respectful of Privacy and Civil Liberties:** Include protection for privacy and civil liberties based upon the established privacy and civil liberties policies, practices, and frameworks.
- **Globally Relevant:** Integrate international standards to the maximum extent possible, keeping the goal of harmonisation in mind wherever possible.

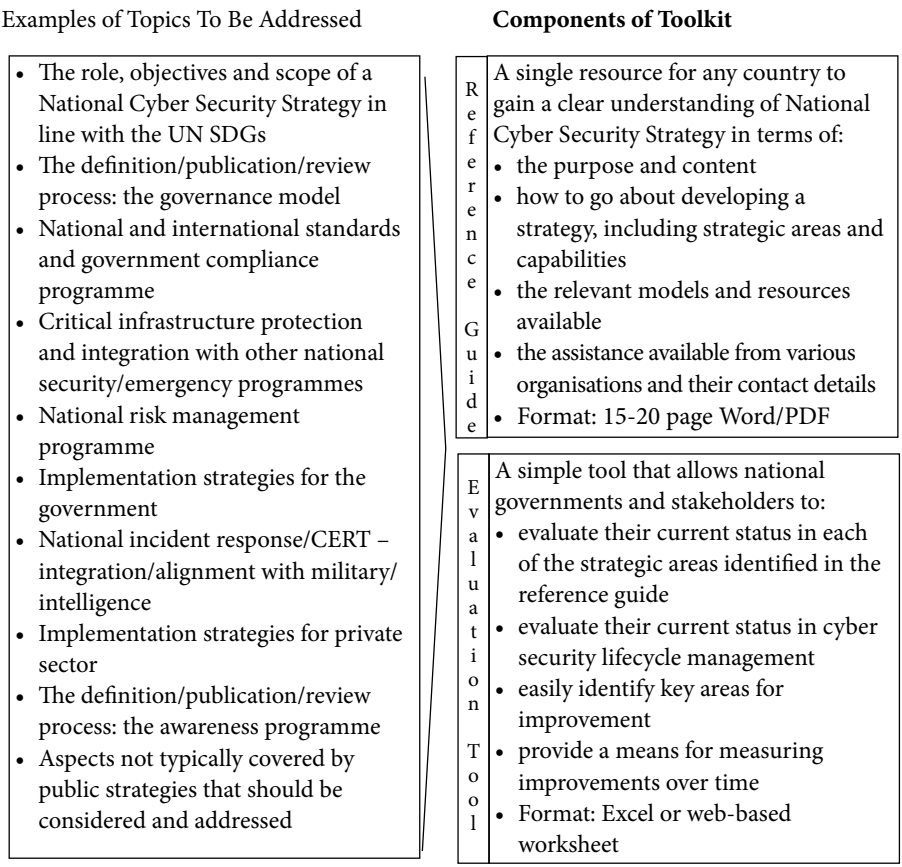
One of the Israeli think-tanks has suggested the following process for cyber security strategy making.[6]

**Fig 4: Boundaries of the Policy and Strategy Papers on a National Level**



The International Telecommunication Union (ITU) has suggested the heading and contents for a Draft National Cyber Security Strategy.[7] The suggested toolkit is given below (Fig 5).

**Fig 5: A Toolkit to Help States to Develop National Cyber Security Strategies**




**Jurisdiction Issues**

There is a conflict of interest as to who is overall responsible for cyber security in most countries. In the USA, the Department of Defence (DoD) is responsible for cyber attacks originating abroad and for protecting DoD networks, while the Department of Homeland Security (DHS) is responsible for coordinating protection of domestic civilian infrastructure. However, many cyber attacks originate from abroad and have the potential to disrupt critical infrastructure.

Responding to cyber attacks is a difficult task for the DHS because it operates without the requisite authority that would allow it to dismantle a foreign actor's network operations. In addition to these legal complications, the DHS does not have the same degree of cyber operations competency as the DoD.

Information sharing between the government and industry has always been a key component of strengthening a country's resilience to hacking campaigns by foreign governments, criminals and hacktivists and non-state actors. However, while industry is responsible for sharing instances of breaches, there are proprietary, privacy and reputational considerations that can inhibit their willingness to do so freely. There are also major inhibitions to the free flow of information from the government to industry – most notably the risk of compromising intelligence sources and methods.

The presence of government bodies such as DHS that insulate intelligence agencies from industry is notable. James Clapper, the former Director of National Intelligence of the USA argues "The DHS is the appropriate storefront and that's the way it ought to be. I don't think the spy crowd should be directly engaging with the private sector."

The division of responsibilities for national cyber security in the USA are as follows:

- The Justice Department would, among other things, "Investigate, attribute, disrupt and prosecute cyber crimes; lead domestic national security operations and conduct domestic collection, analysis and dissemination of cyber threat intelligence;"
- The DHS would, among other things "coordinate the national protection, prevention, mitigation of, and recovery from, cyber incidents; disseminate domestic cyber threat and vulnerability analysis and protect critical infrastructure;"
- The DoD would "defend the nation from attack; gather foreign threat intelligence and determine attribution and secure national security and military systems."

This is precisely what the United Kingdom is seeking to do with its new National Cyber Security Centre (NCSC), which is revamping the way British intelligence agencies collaborate with private industry, by leaning toward more open and direct exchanges to help secure the UK against cyber attacks. Chris Inglis, the former Deputy Director of the NSA, argues that the UK has proposed to "radically transform collaboration between intelligence agencies and the private sector." Practically, this has meant bringing in some 650 people from the Government

Communications Headquarters (GCHQ), the UK's primary signals intelligence agency, and having them work directly alongside industry partners.

**Cyber Deterrence**

The US government published its policy on cyber deterrence in 2015. It has a two-pronged approach that includes "deterrence by denial" and "deterrence by cost imposition." The deterrence by denial approach encompasses defence, resilience, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimise the impact of attacks; together with strong partnerships with the private sector to promote cyber security best practices, assist in building public confidence in cyber security measures, and lend credibility to national efforts to increase network resilience. The "deterrence by cost imposition" line of effort includes, but is not limited to, pursuing law enforcement measures; sanctioning malicious cyber actors; conducting offensive and defensive cyber operations; projecting power through air, land, sea, and space; and, after exhausting all available options, using military force.[8]

***Guiding Principles for Cyber Deterrence***

- The cyber deterrence posture must include both deterrence by denial and deterrence by cost imposition, with a different balance depending on the perpetrator and the severity of the attack to be deterred.
- Deterrence by cost imposition requires understanding what key adversary decision-makers value, holding that which they value at risk, and communicating (explicitly and/or implicitly by precedential action) the credible will and capability to respond.
- Deterrence by cost imposition requires credible response options at varying levels of conflict.
- In the event of a cyber attack (a failure of cyber deterrence), the question should not be whether to impose costs in response, but how and when to do so against the attacker and how to connect the response to the attack.
- The nation must clarify, first, internally, and then to potential adversaries, that it seeks to deter and will aim to impose countervailing costs in response to some forms of costly cyber intrusions.
- Responding to adversary cyber attacks and costly cyber intrusions carries a risk of escalation (and intelligence loss), but not responding carries near certainty of suffering otherwise deterrable attacks in the future.
- Reducing the vulnerability of critical infrastructure is essential not only for

deterrence by denial, it also reinforces the credibility of threats to impose costs on attackers.

Some experts say that the Sony Pictures Entertainment attack, the hack of the US Democratic National Committee and the takedown of the Ukrainian power grid represent failures of deterrence. The unique features of cyber capabilities—versatility, low cost, vast range, high speed, and difficulty of detection and attribution—can be used to support a wide range of national policies, including deterrence and coercion to influence an extensive array of adversarial activities.

***Cyber Defence***

The primary objective of a national cyber defence strategy is:

- To maintain the state's functional continuity.
- To enable the relevant authorities to decide upon, and implement, operations against enemies in the cybernetic and kinetic space, with confidence in the state's ability to withstand a cyber attack.

There are basically three types of cyber attacks:

- Advanced Persistent Threat (APT) – penetration into the depth of an organisation's computer system.
- Rapid, superficial attack, which has immediately recognisable results, and aims to change the site or prevent access to it and to the services it provides in the cybernetic space [defacing, Distributed Denial of Service (DDoS)].
- Infrastructure attack – by damaging hardware components.

For preventing and defending against the three types of attacks, the following are recommended:[9]

- Construct the system with a combination of tools and capabilities that do not require previous information and knowledge of attack components and methods, with an advanced capabilities system based on previous knowledge, specifically for defence against APT attacks.
- Implement inter-organisational information exchange of reports on attacks.
- Formulate a continuous and broad national cybernetic status assessment by organisations such as a national Computer Emergency Response Team (CERT).

- Establish rapid response teams, using research and data on attack tools and attack groups.
- Cooperate with commercial defence and intelligence organisations, as well as international bodies.
- Develop ongoing intelligence collection about enemies and opponents for the purpose of warning.
- Formulate a plan for cybernetic response as part of a possible means of deterrence.
- Develop the ability to recover from an attack when possible, with the understanding that the line of defence is bound to be breached, and, thus, the state must organise for rapid recovery following successful enemy attacks.
- For superficial attacks, establish the ability to recover rapidly and provide the bandwidth that overcomes blocks, by integrating with internet suppliers in the civilian sector.
- Use ability to rapidly transfer attacked sites to alternative, temporary host sites.
- Establish a national capability for analysing hardware attacks due to the technological difficulty of identifying hardware attacks. This should be done in parallel to the use of locally manufactured hardware in cases requiring an exceptional level of security.

***Resilience***

Because defences against cyber intrusion and attack are not perfect, and the spread of offensive capabilities cannot be blocked with confidence, states and major private enterprises must invest in resilience. The general aims are to decentralise potential points of failure or loss, to deploy back-up capabilities and plans, to prepare users of systems for the possibility of disruption and to plan contingencies accordingly. While resilience may deny attackers the gains they seek, pursuing it runs counter to normal economic logic.

**Active Defence**

Active defence is a term that captures a spectrum of proactive cyber security measures that fall between traditional passive defence and offence. These activities fall into two general categories, the first covering technical interactions between a defender and an attacker. The second category of active defence includes those operations that enable defenders to collect intelligence

on threat actors and indicators on the internet, as well as other policy tools (e.g. sanctions, indictments, trade remedies) that can modify the behaviour of malicious actors. The term active defence is not synonymous with "hacking back" and the two should not be used interchangeably.

Activities that produce effects solely within an actor's own networks are referred to as passive defences. They primarily involve the use of perimeter-focussed tools like firewalls, patch management procedures and anti-virus software. These can be installed and left to function independently. Passive defences can also include procedures like white or blacklisting and limiting administrative authorities. While passive defences are necessary for a sound cyber security regimen, they are insufficient by themselves to defend against the most advanced cyber aggressors.

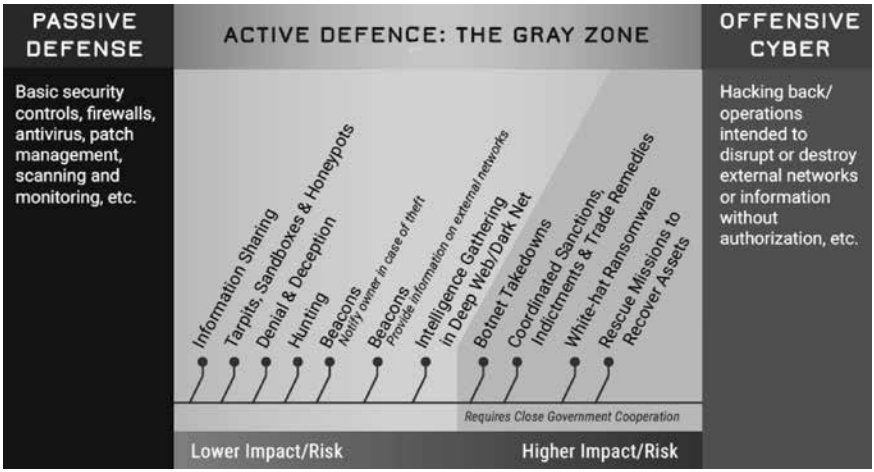
On the other extreme are those activities occurring outside the actor's network, that are aimed at coercing action, imposing costs, degrading capabilities or accessing protected information without authorisation; these could be characterised as offensive. "Hacking back" to retrieve or delete stolen data or to gain information about an attacker's tools, techniques, procedures, and intents fits into this category, as would a retaliatory DDoS attack, the exploitation of a system to extract intellectual property, or the use of malware to damage a system, such as in the case of the Stuxnet.

Examples of active defence measures can be found in Fig 6, and are ranked according to their relative impact and risk from left to right. The activities towards the far left of Fig 6 are relatively common and low risk active defence options such as information sharing and the use of honeypots.

Towards the middle of the active defence spectrum are activities that carry more risk, in that they generally involve operations outside of one's network, and have the potential to lead to minor collateral damage or privacy concerns if used without the requisite level of precision.

Those active defence activities that approach the rightmost extreme of the spectrum in Fig 6 are the most aggressive. Private entities should only utilise such measures, as the figure suggests, when working in close cooperation with the government.

**Fig 6: Active Defence: The Gray Zone**




**Critical Infrastructure Protection**

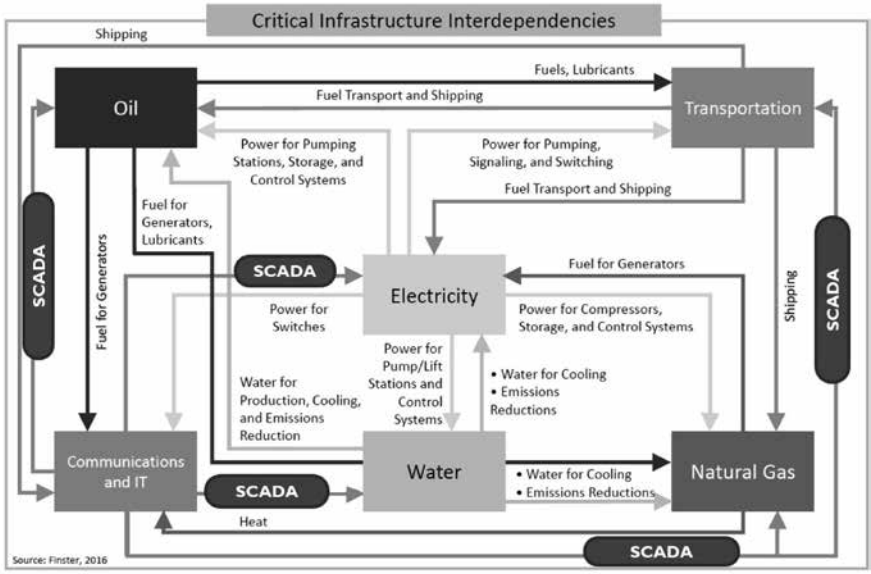
In India, in Section 70 of the Information Technology (IT) Act 2000, Critical Information Infrastructure (CII )is defined as: "The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety." The National Critical Information Infrastructure Protection Centre (NCIIPC) of the National Technical Research Organisation (NTRO) is the nodal agency under Section 70A(1) of the Information Technology (Amendment) Act 2008 for taking all measures, including associated Research and Development (R&D) for the protection of CIIs in India. The National Critical Information Infrastructure Protection Centre (NCIIPC) was deemed to be created by a Gazette notification with specific responsibilities for protecting all CII. While the law was amended in 2008, it would take six years before the NCIIPC was formally created through a Government of India Gazette notification in January 2014.

All businesses face the threat of cyber attacks on their business networks, customer accounts, communication systems, websites, and proprietary data. Many critical infrastructure companies face additional threats to their Operational Technology (OT) systems—often called ICS or Supervisory Control and Data Acquisition (SCADA)—which operate physical processes such as the generation, processing and delivery of power, water, fuels, and chemicals; and the controls for communication and transportation. Cyber attacks on the

OT can potentially disrupt vital services, damage critical equipment, threaten human health and safety, and trigger disruptions in other sectors.

Fig 7 below shows the interdependencies between critical infrastructures:

**Fig 7: Interdependencies Compound Cyber Risks**




**Learning from Best Practices**

The National Security Council (NSC) of the USA tasked the President's National Infrastructure Advisory Council (NIAC) with examining how federal authorities and capabilities can best be applied to support cyber security of high risk assets.

The NIAC recommended the following:[10]

- Establish **separate, secure communications networks** specifically designated for the most critical cyber networks, including the "dark fibre" networks for critical control system traffic and the reserved spectrum for backup communications during emergencies.
- **Facilitate a private sector led pilot of machine-to-machine information sharing technologies**, led by the electricity and financial services sectors, to test public-private and company-to-company information sharing of

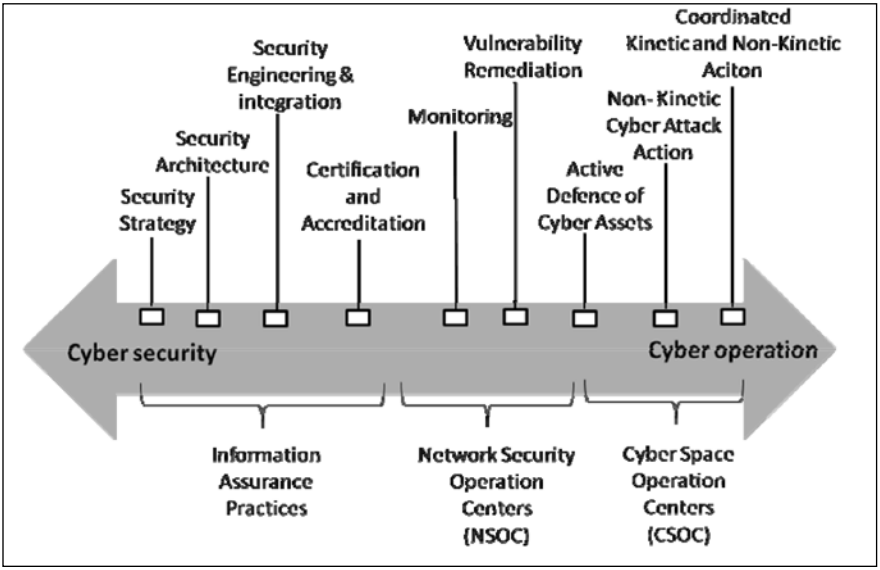
cyber threats at network speed.

- Identify the best in class **scanning tools and assessment practices**, and work with owners and operators of the most critical networks to scan and sanitise their systems on a voluntary basis.
- Strengthen the capabilities of **today's cyber workforce** by sponsoring a public-private expert exchange programme.
- Establish a set of **limited time, outcome-based market incentives** that encourage owners and operators to upgrade cyber infrastructure, invest in state-of-the-art technologies and meet industry standards or best practices
- Streamline and significantly expedite the **security clearance process** for owners of the nation's most critical cyber assets, and expedite the siting, availability and access of Sensitive Compartmented Information Facilities (SCIFs) to ensure that cleared owners and operators can access secure facilities within one hour of a major threat or incident
- **Pilot an operational task force of experts in government and the electricity, finance, and communications industries**—led by the executives who can direct priorities and marshal resources—to take decisive action on the nation's top cyber needs with the speed and agility required by escalating cyber threats
- **Use the national level GRIDEX IV Exercise (November 2017) to test** the detailed execution of federal authorities and capabilities during a cyber incident and identify and assign agency specific recommendations to coordinate and clarify the federal government's unclear response actions.
- Establish an **optimum cyber security governance approach** to direct and coordinate the cyber defence of the nation, aligning resources and marshaling expertise from across federal agencies.
- Task the National Security Advisor (NSA) to review the recommendations included in this report and within six months **convene a meeting of senior government officials** to address barriers to implementation and identify immediate next steps to move forward.

**Offensive Cyber Operations (OCOs)**

The continuum of cyber security and cyber operations is explained in the following Fig 8.

**Fig 8 : Continuum of Cyber Security and Cyber Operations**




The use of offensive operations in cyber space raises many important technical, legal and policy questions. Some of these questions involve topics such as capabilities, rules of engagement, doctrine for the use of offensive capabilities, organisational responsibilities and the intelligence community and a host of other topics related to offensive operations. It is likely that behind the veil of classification, these topics have been discussed at length.

Policy regarding the use of offensive operations in cyber space is generally classified. According to a variety of public sources, US policy regarding offensive operations in cyber space includes the following points:

- The United States would respond to hostile acts in cyber space as it would to any other threat to the nation, and reserves the right to use all necessary means—diplomatic, informational, military and economic—as appropriate and consistent with applicable international law, in order to defend the nation, its allies, its partners, and its interests.
- The laws of war apply to cyber space and because the United States has made a commitment to behaving in accordance with these laws, cyber operations conducted by the United States are expected to conform to the laws of war.
- Offensive operations in cyber space offer "unique and unconventional capabilities to advance US national objectives around the world with little

or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."

- Offensive operations likely to have effects in the US require presidential approval, except in emergency situations.
- Cyber operations, including offensive operations, that are likely to result in significant consequences (such as loss of life; actions in response against the US; damage to property; serious adverse foreign policy or economic impacts) require presidential approval.

However, despite public knowledge of these points, the United States has not articulated publicly a military doctrine for how cyber capabilities might be used operationally. The US' approaches to using nuclear weapons were publicly discussed during the Cold War.

Using offensive cyber operations can cause escalation. But the escalation dynamics of conflict in cyber space are not well understood. Escalation at the tactical level is easy. Once an uncertain threshold is breached, the potential is great for rapid escalation, especially if the breach is substantial. How far can one go before instability occurs? Major strategic/economic attacks are very risky and likely to lead to all out strategic conflict. How would escalation unfold? How could escalation be prevented (or deterred)? Theories of escalation dynamics, especially in the nuclear domain, are unlikely to apply to escalation dynamics in cyber space because of the profound differences between the nuclear and cyber domains. Some of the significant differences are:

- Attribution is much more uncertain.
- The ability of non-state actors to interfere in the management of a conflict.
- The existence of a multitude of states that have non-trivial capabilities to conduct cyber operations.

Guidelines for formulating an attack strategy:[11]

- Security organisations should be required to integrate tools for cyber attacks in their operative plans and in the actual use of force in battle, in both emergency and routine situations.
- Cyber attack ability should not stand alone, but rather should be part of a general plan in order to influence a comprehensive, overt conflict.
- If integrated within a general plan, an effective cyber attack may be implemented against a focussed target through a superficial, rapid, broad attack of objectives other than "gold targets" (military targets, state infrastructure).

- An effective attack need not be a sophisticated attack. A cyber attack can significantly harm a target that is not "cyber rich" and technologically developed. A highly developed technological state may be more vulnerable to a cyber attack than an underdeveloped one because it has fewer defence abilities.
- A state can implement effective cyber attacks through proxies without taking responsibility as part of an overt war, while the state accepts responsibility for the kinetic aspect.
- A significant cyber attack requires build up of force, knowing the target and advance planning.
- Attackers should be integrated within the country's cyber defence system, as part of the regular planning and operation of the defence system.
- A cyber attack can serve as a layer in inter-state dialogue, with the goal of the attack being to send a message, usually a warning.

**Fig 9: Phases of the Intrusion Kill Chain**[12]


**Cyber Capabilities at Operational and Tactical Levels (Corps HQ and Below)**

These can be considered as tactical cyber operations. Armed forces all over the world are developing strategies to seamlessly incorporate actions in the cyber space domain with activities in the traditional war-fighting domains of land, air, maritime and space.[13]

What is our policy to provide cyber capabilities at the operational and tactical levels? In the USA, for carrying out sophisticated cyber operations in the operational and tactical battlefields where proximity to the target is essential, teams from the most elite and niche technology cyber warfare experts of the Tailored Access Operations (TAO) of the NSA are embedded with te appropriate level in the battlefield. Do our armed forces have similar arrangements with the NTRO? We may follow the example of the US Marine Corps and its efforts to get SIGINT and cyber support from the NSA.

Cyber operations in the tactical battle area may include the following:

- Collecting intelligence by rapidly exploiting captured digital media.
- Countering and exploiting the adversaries' unmanned aerial systems by exploiting data feeds.
- Protecting friendly unmanned aerial systems operating in the area of operations.
- Gaining access to closed networks in or near the area of operations, including extracting and injecting data.
- Using electronic warfare systems as "delivery platforms for precision cyber effects".
- Exploiting new devices emerging from new trends and opportunities.
- Conducting cyber space Intelligence, Surveillance, and Reconnaissance (ISR) operations.
- Engaging in offensive social media operations.

Traditional Offensive Cyber Operations (OCOs) missions are conducted against strategic targets and have typical mission timeframes lasting weeks, months or even years. Strategic targets require long lead times to identify vulnerabilities, develop capabilities to exploit these vulnerabilities and execute missions against these targets. The lengthy duration of strategic operations allows extensive testing and verification of these payloads to minimise potential for collateral damage. The rapid pace of operations at the tactical level greatly limits the extensive, in depth planning characteristic of traditional OCOs against strategic targets. In contrast, targets at the corps and below level are typically opportunistic or time sensitive, greatly accelerating the cyber kill chain reconnaissance, weaponisation, delivery, exploitation, installation, command and control and actions on objective.

While OCOs conducted to support corps and below operations may provide the desired effects at the tactical level of war, there is potential for this

OCO support to have significant negative strategic, operational and tactical ramifications. A primary concern of the conduct of OCOs at the tactical level is how operations with potentially strategic effects can be executed in the rapid, decentralised manner required by the breakneck Operational Tempo (OPTEMPO) typified at the tactical level of war. These unintended consequences can include the loss of capability, loss of adversary network access in other geographic combatant commands, risk of digital fratricide, and risk of adversary retaliation. An additional concern is the lack of experience of tactical commanders and their staff in the execution of OCOs in support of corps and below operations, which could also lead to unanticipated and unintended consequences.

An OCO conducted to support corps and below holds the potential to be a non-kinetic, digital panacea capable of temporarily disabling enemy weapon systems and critical infrastructure, to minimise death and destruction on the modern battlefield. Alternatively, an OCO conducted to support corps and below could open wide a digital Pandora's Box of unforeseen and unexpected events unleashed at the speed of cyber on ill-prepared strategic, operational and tactical environments. Given the tremendous resources devoted to developing and procuring OCO capabilities by nation-state and non-state actors, there is a need of considerable analysis and study before getting into such activities at the tactical level.

**Information Operations**

Information Operations (IOs) are defined as actions taken by organised actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion. Cyber operations comprise a subset of information operations.

The various elements of information operations should be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations. Cyber operations can enhance Psychological Operations (PSYOPs) in other ways. Devices and websites both can be infected to introduce users to propaganda that shows up in unexpected places or carries unexpected credentials. Expertise in sensors, emitters, content, and code (for ISR, EW, PSYOPs, and cyber operations, respectively) hardly resembles one another. Each calls for different equipment and training; there is scant reason for them to be organised together.

Information warfare is relatively new and has several advantages:[14]

- It is inexpensive and easy to disseminate the information to a wide audience. Even small groups can have a loud voice.
- This form of warfare is often legal and can reach international audiences, and it is not difficult for the attacking actor to remain anonymous.
- Marginalised communities can locate one another and join forces to become more powerful. For example, automated Twitter accounts can amplify messages.
- Information warfare and influence operations take advantage of the advertised features of information technology, whereas cyber war takes advantage of the virtues of information technology.

***Social Media***

While information operations have a long history, social media platforms can serve as a new tool of collection and dissemination for these activities. Through the adept use of social media, information operators may attempt to distort public discourse, recruit supporters and financiers or affect political or military outcomes. These activities can sometimes be accomplished without significant cost or risk to their organisers.

***Fake News***

Fake news comprise the news articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership or deceive.

**The Role of "False News" in Information Operations:**[15] While information operations may sometimes employ the use of false narratives or false news as tools, they are certainly not one and the same. There are several important distinctions:

- **Intent:** The purveyors of false news can be motivated by financial incentives, individual political motivations, attracting clicks, or all the above. False news can be shared with or without malicious intent. Information operations, however, are primarily motivated by political objectives and not financial benefit.
- **Medium:** False news is primarily a phenomenon related to online news stories that purport to come from legitimate outlets. Information operations, however, often involve the broader information ecosystem, including old and new media.

- **Amplification:** On its own, false news exists in a vacuum. With deliberately coordinated amplification through social networks, however, it can transform into information operations.

**Indian Cyber Space**

The most significant event was the introduction of the Information Technology (IT) Act as early as 2000 and the promulgation of the National Cyber Security Policy by the Ministry of Communications and Information Technology in 2013. The Indian Computer Emergency Response Team (CERT-In) was established in 2004 and continues to act. India has undertaken several steps for the protection, detection and containment of these potentially disruptive attacks against the nation's networks. Initiatives such as Digital India and Smart City and the increasing involvement of the private sector in nation-building endeavours are progressive steps that are also increasing the scope and complexities of cyber security efforts.

The national cyber security policy lacked the following key elements:

- Milestones and performance measures.
- Cost and resources.
- Roles and responsibilities.
- Linkage with other key strategy documents.

India has taken several steps in the recent past to strengthen its cyber defence capabilities. It is time now to enunciate the National Cyber Security Strategy.

**Critical Issues to be Addressed in the Indian Context**

**Command and Control Set-Up:** There should be no ambiguity in the responsibility of organisations for cyber security. In the USA, the National Security Agency and Cyber Command come under the Department of Defence. In the UK, the GCHQ comes under the Foreign Ministry. In Israel, the National Cyber Bureau, directly under the Prime Minister, regulates activity in cyber space. In our context, NTRO has been entrusted with this responsibility which doesn't come under any ministry and operates directly under the Prime Minister's Office (PMO). The interplay between the Ministry of Defence (MoD) and the armed forces, Ministry of Home Affairs (MHA), intelligence agencies, both internal and external, needs to be clearly demarcated. Who will carry out offensive cyber operations in a

conflict scenario: can an intelligence agency do it, keeping in mind the rules of engagement or the laws of armed conflict?

**National Critical Information Infrastructure:** The National Critical Information Infrastructure's Protection Centre (NCIIPC) was formed under National Technical Research Organisation (NTRO). For some selected critical infrastructures, NCIIPC takes the lead role. For other non-critical structures, it is the responsibility of the CERT-In. The National Disaster Management Authority (NDMA) under the MHA also has the responsibility for protection of cyber critical infrastructure. Though, it has done very little on this issue. CERT,-In is an advisory body and not an implementation agency. Responsibility and authority for all the sub-sectors of the critical information infrastructure should be clearly demarcated and made accountable.

The lead agency to formulate a national security polity is the Ministry of Electronics and Information Technology (MeitY). This ministry does not have control over powerful ministries and departments like the MoD, MHA and NTRO. The way our ministries work, in stovepipe systems, the interaction sharing of information, earmarking of specific roles and assignment of responsibility suffer.

We generally follow the US model. The appointment of the National Cyber Security Coordinator directly under the PMO is seen as a positive development: a lot of good work has been done by the National Security Coordinator. However, he does not have any executive power since he is not under any ministry. He is not in the loop for operations undertaken by the intelligence agencies. The staff for the National Cyber Security Coordinator is meagre for a country as huge and diverse as India. In the US, the post of the National Cyber Security Coordinator has been abolished as it was found that this post had become an extra-constitutional authority and was interfering with the routine functioning of the respective ministries responsible for cyber security tasks.

Organisations like the NTRO and National Cyber Security Coordinator are happy to function under the PMO. There is no ministry/legislative control over their functioning. The PMO as such does not have much domain expertise on these niche technology areas. These organisations are protected from routine interference – they have virtual independence. In a way, it is good that they can get things done at a fast pace but there is always a danger of their going overboard and taking unnecessary risks, with grave consequences, when there is no control over them.

**Standards and Protocols:** We need to have uniform standards, protocols and norms across the country in the cyber domain. The agencies involved are MeitY, Indian Standards Institute (ISI)/ Bureau of Indian Standards (BIS) and NCCIPC. Is there a need for a central agency like the National Institute of Standards and Technology (NIST) of the USA functioning under the Department of Commerce?

The Indian IT industry is worth $ 150 billion. It has some well established cyber security procedures. What is the process of exchanging the best practices between this civil sector and the government sector?

There is a serious mismatch of understanding between the civil sector and the government agencies for cyber security. The government agencies feel that the private sector is only interested in grabbing orders but is not serious about developing Indian solutions, does not put in adequate effort in R&D and is not willing to invest in the country's cyber security infrastructure. On the other hand, the private industry feels that there is very little understanding of cyber security in the top echelons of the government agencies, the procedures are too bureaucratic, rigid, long and time consuming and the vendors are usually treated shabbily. It feels that since it provides cyber security solutions across the globe, it has the expertise. The government should approach the private industry and not the other way around, quoting the recent example of the US Secretary of Defence visiting Silicon Valley and interacting with the behemoths for providing support to Department of Defence cyber activities. Surely, there has to be a middle ground where sharply divergent views can meet.

The private industry is very sensitive about any cyber breach in its organisations. It always carries out damage control first and does not like to share the information because of commercial reasons. What can NCCIPC and CERT-In do to develop mutual trust and make sure that this information is shared immediately so that mitigation action across the sectors can be initiated?

In a scenario where a big Indian IT giant has been compromised and data has been stolen and the affected company is reasonably certain about where the attack has come from and carries out a hack back against the party, what should be the role of the government agencies? Though the private industry is duty bound to report any breach of cyber security to the government agencies, a very large number of such incidents go unreported. What is the mechanism by which punitive action is taken against the defaulters?

Regulatory bodies for each sub-sector of the critical infrastructure must be identified and made responsible and accountable for the respective sub-sectors. For

example, if a serious breach in a nuclear power plant takes place, with a potential of great loss to life and property, who should be made accountable? Introduction of private players in the nuclear power sectors will make the issue more complicated. Similarly, who is responsible for the cyber security of the huge defence industrial base or Defence Public Sector Undertakings (DPSUs) and factories under the Ordnance Factories Board (OFB)? With the recent participation of private industries, the cyber security aspects will acquire more relevance. Who is responsible for the cyber security of the private players of the defence industry?

India does not have any credible code breaking capability. Introduction of 128 or 256 bits keys has made the issue of code breaking extremely difficult. However, this capability exists in the NSA of the USA, Government Communications Headquarters (GCHQ) of the UK and probably with Russia and China. If we do not have this capability, then we must make efforts to develop it. Academia, industry and expertise from countries like Ukraine, Belarus and such other East European countries and South Africa can be explored.

**Delay in Implementation of Projects:** After the 26/11 attacks on Mumbai, two very important projects were initiated by the central government on fast track. Both the projects of the National Intelligence Grid (NATGRID) and Central Monitoring System (CMS) have cost and time overruns and are still not complete. NATGRID does not have a linkage to the armed forces.

The National Cyber Security Centre (NCSC), is an organisation of the United Kingdom Government that provides advice and support for the public and private sector on how to avoid computer security threats. It became operational in October 2016, exactly one year after the announcement of its establishment. In India, in principle approval for the National Cyber Coordination Centre (NCCC) was accorded in May 2013, with an initial budget allotment of Rs. 800 crore. On August 08, 2017, the Parliament was informed that only Phase-I of the NCCC had been made operational. When the country has adequate funds and expertise, this type of bureaucratic delay is not acceptable for such projects of national security.

**R&D in the Cyber Security Field**

We have no choice but to have our own software and hardware in niche technology areas as no country shares these. Wikileaks and Edward Snowden have already revealed the capability that the USA has. As an initial effort, Indian researchers should be tasked to develop the same kind of capabilities.

We should take a policy decision to use Indian made switching equipment in our selected critical infrastructure. Indian manufacturers like the Tejas

networks should be encouraged. The human resource development policies must be suitably modified to attract the right kind of talent to train and nurture them. In spite of its huge budget, the NSA is most vulnerable from the insider's threat. Manning and Edward Snowden are the prime examples. The most secret cyber weapons developed by the NSA have been put on the internet and can be used by anybody in the world for cyber operations. What is the policy to thwart the insider threat in our cyber security organisations?

In September 2015, the Indian government released a draft National Encryption Policy that sought to set encryption standards and lay down conditions for decryption of information for lawful investigation. This was hastily withdrawn under pressure from the media. It is time now to catch the bull by the horn. The national security interest must be supreme.

**Armed Forces Domain**

The cyber security of the three Services is not audited by any outside agencies, including the NCCIPC. The three Services don't even audit each other. The respective Services certify themselves as cyber secure. This is not acceptable. Cyber security of the IT network of the three Services must be audited by some external agency. In the USA, professional hackers are called in, in a big bounty programme and challenged to hack DoD classified networks, and awarded huge amounts of prize money. This is how they discover vulnerabilities in their networks. The Indian armed forces must also do something like this.

Within the US DoD, there is a organisation called Defence Information Systems Agency (DISA), which provides, operates and assures command and control and information sharing capabilities in direct support to joint war-fighters, national level leaders and other missions across the full spectrum of military operations. It works under the DoD's Chief Information Officer (CIO). In India, the three Services as well as the MoD do not have CIOs. Should we have an organisation like the DISA in the MoD as a separate organisation and designate it as the CIO of the MoD?

There should be clarity as to what is to be constituted as an act of war in the cyber domain. Factors like loss of life and property, economic impact, diplomatic and political effects can be considered to term such an attack as one of significant consequences.

Who will give permission for offensive cyber operations? What are the rules of engagement?

India procures a huge amount of defence equipment from foreign countries. What is the mechanism to check whether there is any malware in the increasingly sophisticated technology areas. No country shares its codes. What is the mechanism in the procurement of equipment procedure and supply chain management system to ensure that bugs are not present?

The human resource development policies for the armed forces in the cyber domain will require drastic changes to attract and retain talent in such niche technology areas. The present policies are inadequate.

## Space Strategy

### *Preview*

Space was once called the "final frontier." Secure and stable access to space is a key component of our everyday lives. Currently, almost every country either owns a satellite or has a stake in space. There are approximately 1,100 operational satellites in orbit around the Earth, causing some orbital planes to be severely overcrowded. Access to, and the use of, space is a vital national interest. The domain is now "congested, contested, and competitive." The list of human activities that are dependent on space systems contains most of the major functions that are vital to modern society, including trade and commerce; banking and financial transactions; personal, corporate, and government communications; agriculture and food production and distribution; power and water systems; transportation; news gathering and distribution; weather assessment and prediction; health care and entertainment. Were the world to suddenly be "without space," these would all seriously degrade or shut down entirely.

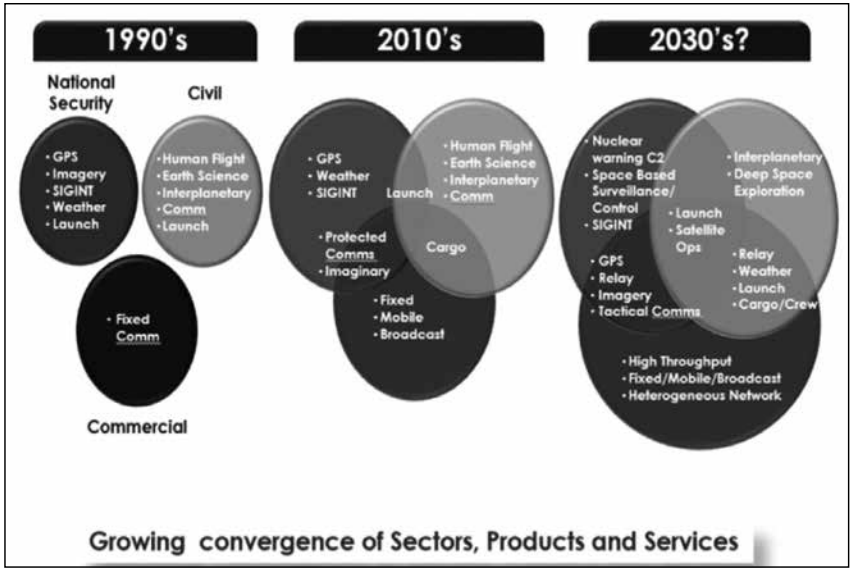
Space is a domain – like the air, land, sea, and cyber space – within which military operations take place. Space is integral to the modern way of warfare. Military forces shoot, manoeuvre, and communicate. Space capabilities compound the speed, precision, accuracy, and clarity of these functions, making the force more lethal at less cost in lives and resources. The first thing satellites do is collect information. Space capabilities have proven to be significant force multipliers when integrated into military operations. Space capabilities provide global communications; Positioning, Navigation, and Timing (PNT) services; environmental monitoring; space-based Intelligence, Surveillance and Reconnaissance (ISR).

**Characteristics of Space:** The space environment has unique characteristics that impact military operations. The characteristics of space include:

- **No Geographical Boundaries**: International law does not extend a nation's territorial sovereignty up to the Earth's orbit. Nations enjoy unimpeded satellite overflight of other nations through space.
- **Orbital Mechanics:** Satellite orbits must follow certain orbital parameters due to the laws of physics. Satellite operators can, in limited circumstances, change a satellite's orbital parameters, which can significantly degrade the performance or life span of a system.
- **Environmental Considerations:** The space environment is a significant limiting factor influencing every aspect of a satellite's size, weight and power affecting the performance and life span of any operational spacecraft.
- **Electro-Magnetic Spectrum (EMS) Dependency:** Space-based assets depend on the EMS as their sole medium for transmitting and receiving information and/or signals. The electro-magnetic frequency bands that space-based systems use are fixed and cannot be changed after launch.

## Evolution of Space Sectors

**Fig 10 : Growing Convergence of Sectors, Products and Services**




## Cyber and Space Capabilities

Multiple countries possess cyber capabilities that could be used against space

systems; however, actual evidence of cyber attacks in the public domain is limited. A growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems. This indicates that manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors.

There is a clear trend toward lower barriers to access, and widespread vulnerabilities, coupled with reliance on relatively unsecured commercial space systems create the potential for non-state actors to carry out some counter-space cyber operations without nation-state assistance. However, while this threat deserves attention and is likely to grow in severity over the next decade, there remains a stark difference at present between the cyber attack capabilities of leading nation-states and those of other actors.[16]

***Threat Pathways***

The threat pathways are hugely complex, but the main strands can be summarised as follows:

- Increasing numbers of individual satellites and constellations providing an ever increasing number of entry points.
- Increasing connectedness through communication paths, and increasing connectedness of satellites while in orbit.
- Autonomous communication paths to billions of devices, with little opportunity for humans to intervene.
- An international supply chain of satellite components, with the associated uncertainties about provenance and standards of production.
- The imperatives of speed to market, forcing designers and manufacturers to skip or pay only passing attention to important security controls.
- Security costs that are disproportionate to the costs of manufacture of smaller and cheaper satellites.
- Back door holes in encryption and otherwise secure control systems.

The methods of the attack could be:

- Jamming, spoofing and hacking attacks on, for example, communication networks, by using space infrastructure;
- Attacks on satellites, by targeting their control systems or mission packages, perhaps taking control of the satellite to exploit its inherent capabilities, shut it down, alter its orbit (perhaps thereby 'weaponising' it), or 'cook'

or 'grill' its solar cells through deliberate exposure to damaging levels of highly ionising radiation;

- Attacks on the ground infrastructure, such as satellite control centres, the associated networks and data centres, leading to potential global impacts (for example, on weather forecasting systems, which use large quantities of space-derived data).

**China's Space Capability**

China is on its way to becoming a space superpower. It has put up sophisticated communications and intelligence satellites, offered cheap launch services to other nations and launched manned mission initiatives. It has also developed a "quantum satellite" designed to transmit quantum encrypted information from space, which is theoretically hack-proof and ensures that any attempt to intercept or tamper with the transmission would alert both the sender and receiver. China is fielding sophisticated satellites that feature Electro Optical (EO), Synthetic Aperture Radar (SAR) and Electronic Reconnaissance (ELINT) sensors. The Beidou is China's satellite navigation system and is intended to reduce China's reliance on the US Global Positioning System (GPS).

In 2007, China shot down one of its old weather satellites in an Anti-Satellite (ASAT) test in Low Earth Orbit (LEO). This incident demonstrated China's ability to disable and destroy the space assets of other countries its determination to have a deterrence and defence policy. These capabilities are broad and growing, and include "direct-ascent anti-satellite missiles, co-orbital anti-satellite systems, computer network operations, ground-based satellite jammers and directed energy weapons."

**India's Space Capability**

The Indian Space Research Organisation (ISRO) has developed a highly successful space programme that has supported many of the national developmental programmes and initiatives. The agency has a civil mandate and the emphasis has been on the use of space technology for societal and economic development. ISRO is operating one of the biggest fleets of satellites (remote sensing, satellite communications and navigation) in the world. In a relatively short time, India's space programme has made significant progress in space launch systems. Moving from one launch, from 1993–2006, India has progressed to a steadily growing number of launches in the past decade. In the same time period, India's launch payloads have grown from 846 kg per year to

7,432 kg. Today, India's space programme is valued at more than $2.3 billion in assets already in orbit; this figure rises to around $37 billion when ground-based infrastructure and value added services are included.

India's growing market share is attributed to its low price for many launches. The Polar Satellite Launch Vehicle (PSLV), India's most frequently used launch vehicle, is estimated to cost approximately $15 million per launch, roughly one-quarter the price of a private US-based launch cost of $60 million. The maximum payload of the PSLV is roughly one-fourth that of a US-based launch vehicle to the same orbit,

Now India is pursuing the development of a Geosynchronous Launch Vehicle (GSLV) and a Reusable Launch Vehicle (RLV). The RLV is in the technology demonstration phase. The RLV will provide India with a fixed wing, reusable vehicle that operates similarly to the former US space shuttle. The RLV programme, if successful, could contribute to India's efforts to reduce costs for space access in two ways: reusability and mass reduction.

India's launch capacity of four to five launches a year and the limited heavy lift capability is a major impediment towards capacity building. Concerted efforts are being made by ISRO towards achieving a launch rate of 16 by the end of the decade. These include augmenting the launch infrastructure, enhancing the capacity of component providers and exploring the option of setting up a third launch pad at Sriharikota. Additionally, technologies matured for the ballistic missile programme could be explored for developing dedicated launch capability for microsatellites.

There are plans to hand over routine Polar Satellite Launch Vehicle (PSLV) operations to a consortium of public and private companies by 2020. This would also allow the country's primary space agency to be freed of expending effort and resources for routine operations and concentrate wholeheartedly on technology development and futuristic space exploration programmes.

**Capacity Building in the Industry:** There is an opportunity for the private sector to participate in space as markets have been opened up and Foreign Direct Investment (FDI) is possible. However, as this was hithertofore only the domain of ISRO, there will be challenges to strike a balance between the two. We must develop and innovative solutions for the defence space system in the private sector.

**Space and Indian Armed Forces:** The Indian armed forces today are increasingly dependent on space-based assets to operate efficiently across the spectrum of operations, from strategic to tactical, from nuclear to sub-conventional and from Out of Area Contingencies (OOACs) to disaster

management. They provide the advantage of large geographical coverage, access to inhospitable and remote areas and invulnerability to ground-based attack systems. Space-based capabilities are being integrated into the concept of operations and operational plans of the advanced militaries all over the world.

India's space organisation is fundamentally focussed on exploiting space for peaceful purposes with a limited set of national security objectives now embedded in the larger civilian effort. Formation of a dedicated defence space establishment in India is a logical conclusion. The Government of India accepted the expanding strategic and tactical level operational demands of the armed forces by instituting the Integrated Space Cell (ISC) within the Integrated Defence Services (IDS) in February 2008. The ISC has a coordinating role between the armed forces as well as with the Department of Space, ISRO and Ministry of Defence for greater integration of space technology and assets into military operations. Following such developments, ISRO built and launched the dedicated military communications satellites, GSAT- 7 (2013) for the Navy and GSAT-6 (2015) for the armed forces. Further, the Technology Perspective and Capability Roadmap (TPCR) of the IDS details several space-based capabilities envisioned for India's expanding space-based security needs.[17]

There is a proposal for the creation of a Defence Space Agency (DSA) as an interim arrangement until a full-fledged dedicated Space Command is raised. The present ISC can be the nucleus for the proposed Space Command as and when it is raised.

There is a need to make a Standard Operating Procedure (SOP) for coordination of space users such as a Defence Image Processing and Analysis Centre (DIPAC) under the Defence Intelligence Agency (DIA), Aviation Research Centre (ARC), National Technical Research Organisation (NTRO), Defence Satellite Control Centre (DSSC) and Research and Analysis Wing (R&AW).

There is a need of auditing and accounting of technological, technology integration and performance. A dedicated task force consisting of representatives of academia, industry, armed forces, think-tanks and ISRO can be formed.

**Role of Private Sector**

While the Indian space programme is entirely state-driven, ISRO is around 70-80 percent reliant on private sector contractors for components and services. There is a huge number of Indian companies providing ISRO with launch and satellite components—the leaders being established engineering

and technology firms such as Larsen & Toubro, Walchandnagar Industries, and Godrej, with Tata Aerospace gaining ground. There is also a whole range of new space actors emerging, including several start-up companies based in Bangalore and elsewhere. Most of them are in the small satellite segment, but there are one or two companies talking to ISRO and the larger space community about developing launching capabilities for slightly bigger satellites. ISRO should finalise a policy that facilitates greater private sector participation, particularly in a role beyond that of component supplier.

There have been increasing calls for allowing private sector firms to manage some of the tried and tested programmes, which would allow ISRO to refocus on the larger, more ambitious interplanetary missions, as well as purely research-oriented programmes. For example, the former ISRO Chairman called on Larsen & Toubro to take over India's Polar Satellite Launch Vehicle (PSLV) programme, which has been an established programme for more than a decade now. Privatisation may also allow India to increase its launch capacity, which is currently at four to five per year and compares poorly with the twenty or so launches China does on average. Increasing the number of launches is partly an infrastructural problem tied to the number of launch facilities in India, but ISRO also has internal constraints on its capacity to deliver.[18]

**Space Capabilities Required**

**Signals Intelligence:** Satellites can monitor various types of activities in the electromagnetic spectrum. Some listen to radio traffic, collecting Communications Intelligence (COMINT). Others are able to detect and record electronic signals, collecting Electronic Intelligence (ELINT). COMINT and ELINT together are referred to as Signals Intelligence (SIGINT). SIGINT today also includes capturing of telemetry signals, with emphasis on missiles. The ground-based SIGINT equipment has inherent limitations due to radio line of sight and threat of equipment getting compromised. SIGINT payloads on an elevated platform like a satellite would boost the capability tremendously. Presently, India has very limited space-based SIGINT capability. India should establish ISR capability to monitor activities in the Indian Ocean Region (IOR) and Tibet Autonomous Region (TAR).

**Navigational Capabilities:** The Indian Regional Navigation Satellite System (IRNSS) constellation provides accurate position information to users in India as well as the region extending up to 1,500 km from its boundary. This constellation can be used to aid in navigation for missions on land, at sea and

in the air. For the ballistic missile programmes such as the Agni and the cruise missile programme such as the BrahMos, we have no choice but be self-reliant.

**Counter-Space Operations and ASAT Capabilities**

Counter-space operations will not necessarily be anti-satellite systems shooting down satellites, although a number of nations have tested anti-satellite capabilities in recent years. Because space operations depend on ground-based facilities to control the satellites and obtain data from them, there is a significant terrestrial component to space operations. Similarly, both the systems that control satellites and the data that flow over satellite networks are vulnerable to cyber attacks and data manipulation. A hacked satellite that turns off its camera at key moments is as neutralised as a functioning satellite that is intercepted and destroyed by a co-orbital or ground-based anti-satellite system. In future conflicts, both the outer space and information space domains will be central battlefields and operations there will have as much impact as traditional activities in the air, land and at sea .

As a matter of policy, India is against weaponisation of outer space. After the Chinese demonstration of ASAT capabilities, there has been a debate on whether India should also develop ASAT capability. This would act as a deterrent against adversaries in the future. India's stand on ASAT tests is not clear. There is a feeling in the strategic security circles that if India does not demonstrate this capability now, it will be left behind at the space high table as happened in the nuclear domain.

While India does have the fundamental building blocks for a kinetic kill, full-fledged ASAT weapon based on the Agni and the ballistic missile interceptor, showcasing this capability has to be done in a responsible manner, without creating a huge amount of long lasting debris that could damage existing satellites.

**Space Situational Awareness**

It is necessary to have military Space Situational Awareness (SSA) capabilities to not only track objects in space but also map the capabilities of various space systems and their implications for national security. Today, no country that aspires to be counted can afford to ignore the power that comes about through a robust SSA and a C4ISR capability in which space assets will play the key role. Once a country has a strong SSA and C4ISR capability, it can choose to use this as a force multiplier for either a proactive (offensive) or reactive (defensive)

strategy. India now has limited capabilities in the field of space situational awareness, with the major work for tracking objects such as space debris being carried out by ISRO's Multi-Object Tracking Radar (MOTR).

The measures towards assured access would include protection measures to defend space systems against diverse threats, incorporating resilience and redundancies in the systems' architecture and also responsive capabilities for quick replacement of lost or damaged satellites. A critical element of securing own interests is the ability to monitor the various activities within the domain. Current Indian SSA capability is highly inadequate for space security functions. There is a necessity to gradually develop SSA capability by building terrestrial radar and optical sensors and the supporting computing and analytical ground infrastructure.

SSA and a robust C4ISR are the main pillars around which a space strategy for the country has to be formulated. Achieving parity in SSA and C4ISR with other major players is a major priority. The technology gaps will have to be addressed, along with the organisational and institutional bottlenecks.

**Capability Development in Niche Space Technology Areas**

**Hypersonic Glide Vehicle (HGV):** HGV technology could be a revolutionary transformation overriding existing ballistic and cruise missile capabilities. Traveling at hypersonic speeds, HGVs reduce the defending party's response time. In addition to improved speed, their considerable mobility and range allow HGVs to overcome or circumvent existing missile defence systems. Even if an HGV is within range of current missile defence interceptors, its speed and agility will challenge the computing programmes used to plot the course for an interceptor. Missile defence sensors and interceptors are often intended to defend against threats from one direction. HGVs could have the range to approach targets from a wider series of azimuths, negating current missile defences. Collectively, when compared to traditional intercontinental ballistic missiles, the advantages provided by HGVs give them a greater penetration capability.

China's HGV programme has been concentrated in ground-launched capabilities. Its prototype HGV apparently is the WU-14, also known as the DF-ZF. Beijing could use the WU-14, or a modified version, on multiple ballistic missile systems. In recent months, it has reportedly conducted multiple HGV tests with the DF-17, a medium-range ballistic missile with an estimated range between 1,800-2,500 km. China's developmental DF-41, with a range of at least

12,000 km, may be able to carry multiple WU-14 HGVs. China's emerging HGV programme threatens not only the US but also countries such as Japan and India.

India must take note of this development and initiate appropriate actions to develop similar capability.[19]

Apart from these requirements for satellites and launchers, there is a number of technology areas that may require development. Some of these critical areas are:

- ELINT technology development.
- Infrared technologies and imaging sensors.
- Improved integrated optics for imaging sensors.
- Synthetic Aperture Radar(SAR) weight reduction initiatives.
- Small satellites related developments.
- Data processing especially SAR data processing.
- Use of commercial open source data for strategic work.
- Tracking Data Relay Satellite System (TDRSS), compatibility related developments.

There is also a number of technology areas where Indian capabilities have to be significantly enhanced to meet medium and longer term anticipated needs. These include:

- Ion propulsion.
- Satellite-to-satellite and satellite-to-ground laser communications.
- Secure communications.
- C4 network operations integration of space and other networks.
- Networked LEO communications satellite systems architecture and design.
- Operational use of the GSLV Mark 3.

**Requirement of Space Strategy**

Traditionally, the scientific and technological bureaucracy was left to set its own goals and achieve whatever it could. The political leadership failed to take ownership of this particular domain. The government needs to set goals, requirements, and milestones outlining where India wants to be in 2020 and 2030. The scientific bureaucracy's responsibility should be to achieve those goals. However, only the two scientific organisations of space and atomic energy have made India proud by achieving world class standards. Coincidentally, both departments work directly under the Prime Minister, and the Chairmen of ISRO and the Atomic Energy Commission are the ex officio secretary of

the respective department. After the Indian Mars Orbiter mission successfully deployed its orbiter, earning the state a huge amount of positive publicity, Prime Minister Modi began to attach much more importance to space programmes and has been focussing more high level attention on the domain. Last year, the induction of India's Foreign Secretary to the Space Commission for the first time confirmed India's focus on space from a foreign policy and national security perspective.

India has mastered the art of accomplishing big space missions with small budgets, which has been done by combining innovative tactics and prudence. It is time for India to pay attention to other aspects of its space policy, and seriously think through its future needs in outer space in a more competitive environment. It is time for India to outline a national level space policy that is all-encompassing. Such a policy framework must be initiated by the political leadership, may be from the Prime Minister's Office. Such an all-inclusive policy framework should not be issued by ISRO alone because then the mandate of such a policy outline will be limited to civilian and peaceful aspects of space. The domain of outer space has undergone significant changes in the last decade and space is now an integral part of militaries around the world. India cannot afford to ignore those realities even as it prefers outer space to be a peaceful domain.

India has many external security challenges in the form of a two-front war and internal security challenges. The internal security challenges consist of cross-border terrorism, including attacks on cities like Mumbai, on sensitive military installations like in Pathankot and Uri, and for surveillance on Left Wing Extremism (LWE) infested areas. There is a requirement of our space capabilities for surveillance of our cross-border areas, vast coastline and water spaces and LWE affected areas. The importance of this capability for offensive operations like surgical strikes needs no elaboration.

Till date, India's approach for utilisation of space for strategic and security purposes has been low key. India has used some of the space assets within legally accepted limits of the Outer Space Treaty (OST). ISRO has very strict firewall rules to cordon off civilian space assets for fear of restrictions being imposed by the world powers.

Today, India is a major space power. However, India's space strategy has not been articulated or published. India must categorically announce its space strategy. It should factor in the growing requirement of space assets in the social, economic and security areas. The National Space Strategy should include:

- Command and control structures for offensive and defensive use of space and maintenance of space deterrence. Which agency or agencies would control which activity should be clearly spelt out.
- Our stands on anti-satellite weapon, space situational awareness and the international code of conduct.
- Under what circumstances offensive use of space will be undertaken. This would bring clarity to the minds of both adversaries as to what might provoke a military response in terms of jamming, blinding, destruction and interference.
- How space assets will be used to deal with India's internal security challenges.
- Cyber challenges to outer space to be factored in.

The responsibilities of India's Space Command, when raised, may include the following:

- Planning and conducting military space operations.
- Advocating for space capabilities.
- Representing Indian military space interests internationally.
- Assisting human spaceflight operations.
- Providing warning and assessment of any attacks on space assets.
- Conducting space situational awareness operations that benefit the Indian public and private sectors, human space flight and commercial and foreign space entities.

**Conclusion**

India's space programme has grown enormously over the past decade but without a broad strategic plan. India has lacked an overall National Security Strategy that lays out its long-term goals and objectives. As India's power and influence rise, there has to be greater clarity on what it wants to achieve as a nation in its overall security as well as within each of the important security domains such as nuclear and outer space.

While there are significant opportunities to integrate satellite-based technologies into the defence realm, there is a need to carefully plan this technology integration. Given that the DRDO does not focus its efforts on development of satellite platforms, there is tremendous opportunity for Indian industry to invest into such platforms.

**Overall Deduction**

There is a global trend towards increased instability in the domains as nations develop offensive capabilities. Consequently, space has been labelled as the fourth, and cyber, the fifth, dimension of warfare. The current international legal regime is ill equipped to prevent this weaponisation. The mutual distrust among nations and the unpredictability of non-state actors is thwarting efforts in this direction. In the future, defensive counter-measures might prove to be inadequate to contain the threat. The nation needs to evaluate development and deployment of offensive capabilities along with their supporting structures as part of the deterrence strategy. The armed forces can play an empowered role in these efforts through the establishment of the Space and Cyber Commands.

Land and sea warfare have established bodies of law in the Geneva and Hague Conventions and in the San Remo Protocol, respectively. These rules serve as an agreed upon framework for "acceptable" behaviour in warfare. But what constitutes an act of war in space or cyber space? There is a requirement of deliberate efforts to redefine what constitutes war in the space or cyber space domains.

Both the cyber and space domains are global commons. There is a close integration and dependence between these domains. The armed forces are getting increasingly dependent on both cyber and space domains for fighting an integrated battle. There is a need to evolve a synergistic approach to fight a war in these domains. We must analyse the issues involved deliberately and take appropriate actions at the strategic, operational and tactical levels.

**Notes**

1. US Army Field Manuals FM 3-38, FM 3-12.
2. US Department of Defence Instruction 8500.01, Cyber Security, March 14, 2014.
3. Defence Science Board Task Force Report on "Resilient Military Systems and the Advanced Cyber Threat;" January 2013.
4. "Why We Need to Measure Military Cyber Power," World Economic Forum, March 29, 2018, available at : https://www.weforum.org/agenda/2018/03/why-we-need-to-measure-military-cyber-power
5. Cristin Flynn Goodwin and J. Paul Nicholas, "Developing a National Strategy for Cybersecurity," October 2013, available at https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW5Aly
6. Gabi Siboni and Ofer Assaf, "Guidelines for a National Cyber Strategy," Institute for National Security Studies, March 2016, available at http://www.inss.org.il/publication/guidelines-for-a-national-cyber-strategy/
7. Dr. Frederick Wamala, "The ITU National Cybersecurity Strategy Guide,"

September 2011, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

8. White House Policy Report, "Cyber Defense Deterrence Policy", December 2015.
9. Siboni and Assaf, n.6.
10. "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure," National Infrastructure Advisory Council, August 2017.
11. Siboni and Assaf, n.6.
12. "A 'Kill Chain' Analysis of the 2013, Target Data Breach," Majority Staff Report For Chairman Rockefeller, Committee On Commerce, Science And Transportation, March 26, 2014.
13. Michael Klipstein and Michael Senft, "Cyber Support to Corps and Below: Digital Panacea or Pandora's Box?" October 19, 2016, available at http://strategicstudyindia.blogspot.com/2016/11/cyber-support-to-corps-and-below.html
14. "Emerging Trends and Methods in International Security: Proceedings of a Workshop," The National Academies Press, 2018.
15. Jen Weedon, William Nuland and Alex Stamos, "Information Operations and Facebook", April 27, 2017, Version 1.0.
16. Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Secure World Foundation, April 2018).
17. "Technology Perspective and Capability Roadmap (TPCR )," Headquarters Integrated Defence Staff, Ministry of Defence, April 2013, available at http://mod.gov.in/writereaddata/TPCR13.pdf
18. Rajeswari Pillai Rajagopalan, "India's Space Program: Challenges, Opportunities, and Strategic Concerns," The National Bureau of Asian Research, February 2016, available at http://www.nbr.org/research/activity.aspx?id=651
19. Davis Florick, "Russian and Chinese Hypersonic Glide Vehicles: Closing the Gap," April 23, 2018, available at https://www.realcleardefense.com/articles/2018/04/23/russian_and_chinese_hypersonic_glide_vehicles__closing_the_gap_113356.html

## Bibliography

US Army Field Manuals FM 3- 38 and FM 3-12.

James Van De Velde, "The Fifth Domain Won't be the Sole Battleground," August 30, 2017, available at https://www.thecipherbrief.com/article/exclusive/tech/fifth-domain-wont-sole-battleground

Patricia Lewis and David Livingstone, "What to Know About Space Security", *Chatham House*, September 27, 2016, available at https://www.chathamhouse.org/expert/comment/what-know-about-space-security

David Livingstone and Patricia Lewis, "Space, the Final Frontier for Cybersecurity?", *Chatham House*, September 2016, available at https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-09-22- space-final-frontier-cybersecurity-livingstone-lewis.pdf

Kazuto Suzuki, "Satellites, the Floating Targets", *The World Today*, February and March 2016.

Madeleine Moon (United Kingdom), "NATO Parliamentary Assembly, Defence and Security Committee for the Space Domain and Allied Defence Draft Report," Sub-Committee on

Future Security and Defence Capabilities, March 20, 2017, available at www.nato-pa.int

Joint Chief of Staffs, "Cyber Space Operations," US Army Joint Publication 3-12, February 05, 2013, available at http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf

"The Department of Defence Cyber Strategy," The Department of Defence, April 2015, available at https://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Report of the Defence Science Board (DSB) Task Force on Cyber Deterrence, February 2017 available at http://www.dtic.mil/get-tr-doc/pdf?AD=AD1028516

From the website of the Prime Minister of Israel, http://www.pmo.gov.il/secretary/govdecisions/2011/pages/des3611.aspx

Gabi Siboni and Ido Sivan-Sevilla, "Israeli Cyber Space Regulation: A Conceptual Framework," *Cyber, Intelligence, and Security*, Vol.1, No.1, January 2017, available at http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/Israeli%20Cyber space%20Regulation%20A%20Conceptual%20Framework,.pdf

Puneet Bhalla, "Investments in the Space and Cyber Realm for India's National Security," *CLAWS Journal*, Winter 2016, available at http://www.claws.in/images/journals_doc/273305959_1742641027_PuneetBhalla.pdf

Cristin Flynn Goodwin and J. Paul Nicholas, "Developing a National Strategy for Cybersecurity Foundations for Security, Growth, and Innovation," October 2013.

Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson and Drew Herrick, "Tactical Cyber: Building a Strategy for Cyber Support for Corps and Below," RAND Corporation Report, available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf .

Col P K Mallick, "Space Warfare an Appraisal," *Pinnacle*, September 2001 issue, available at https://drive.google.com/file/d/0B7lCgXHBh1PaMzBvZnFGZlFFRE0/edit?usp=sharing .

Balraj Nagal, "Space: The Future Pivot of Strategic Stability?," *CLAWS Journal*, Summer 2017.

Kevin Pollpeter, Eric Anderson, Jordan Wilson and Fan Yang, "China Dream, Space Dream : China's Progress in Space Technologies and Implications for the United States," A report prepared for the US-China Economic and Security Review Commission.

Michael Haas, "Vulnerable Frontier: Militarised Competition in Outer Space", *Strategic Trends 2015: Key Developments in Global Affairs, 2015*, http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-Trends-2015-Vulnerable-Frontier.pdf

Kazuto Suzuki, "Satellites, the Floating Targets", *The World Today*, February and March 2016.

For an overview, see Thomas Single, "JAPCC NATO Space Operations Assessment in Particular," 2009, pp.21-30.

Kartik Bommakanti, "A Conceptual Analysis of Sino-Indian Space Deterrence and Space Warfighting," ORF, April 2017, available at http://cf.orfonline.org/wp-content/uploads/2017/04/ORF_OccasionalPaper_SpaceMilitaryStrategy.pdf

Indian Space Research Organisation, "Polar Satellite Launch Vehicle," Department of Space, Government of India, available at http://www.isro.gov.in/launchers/pslv

Ajey Lele, "GSAT-6: India's Second Military Satellite Launched," Institute for Defence Studies and Analyses, August 31, 2015, available at http://www.idsa.in/idsacomments/GSAT6IndiasSecondMilitarySatelliteLaunched_alele_310815

"Vision and Mission Statements," Indian Space Research Organisation, accessed November 05, 2015, available at http://isro.gov.in/about-isro/vision-and-mission-statements

"The Space Report 2015: The Authoritative Guide to Global Space Activity," The Space Foundation, accessed December 21, 2015, available at http://www.spacefoundation.org/sites/default/files/downloads/The_Space_Report_2015_Overview_TOC_Exhibits.pdf

S Chandrasekhar, "The Emerging World Space Order and Its Implications for India's Security," in Subrata Ghoshroy and Goetz Neuneck, *South Asia at a Crossroads: Conflict or Cooperation in the Age of Nuclear Weapons, Missile Defense and Space Rivalries* (Germany: NomosVerlag Publishers, 2010), pp. 219-220.

S Chandrasekhar, "Space, War and Security – A Strategy for India, December 2015," International Strategic and Security Studies Programme, National Institute of Advanced Studies, Bengaluru, India.

Rajeswari Pillai Rajagopalan and Arvind K. John, "A New Frontier: Boosting India's Military Presence in Outer Space," Observer Research Foundation Occasional Paper 50, January 2014, http://www.orfonline.org/cms/export/orfonline/modules/occasionalpaper/attachments/occasionalpaper50_1392021965359.pdf

"Technology Perspective and Capability Roadmap (TPCR)," Headquarters Integrated Defence Staff, Ministry of Defence, April 2013, available at http://mod.gov.in/writereaddata/TPCR13.pdf

Sarah Knapton, "Star Wars: How Future World Conflicts Will Be Decided in Space," *The Telegraph*, December 19, 2015, available at http://www.telegraph.co.uk/news/science/space/12058054/Star-Wars-how-future-world-conflicts-will-be-decided-in-space.html

Rajat Pandit, "India May Get Three Unified Commands for Special Operations, Battles in Space, on Web," *The Times of India*, accessed October 27, 2015, available at http://timesofindia.indiatimes.com/india/India-may-get-three-unified-commands-for-special-operations-battles-in-space-on-web/articleshow/49399708.cms

Xiaodon Liang, "India's Space Program: Challenges, Opportunities, and Strategic Concerns," The National Bureau of Asian Research, February 10, 2016, available at http://www.nbr.org/research/activity.aspx?id=651 .

Dr. R Sreehari Rao, "Space-Based Signal Intelligence Systems: Global Trends and Technologies – Defence Electronics Research Laboratory," accessed April 19, 2016, available at http://indianstrategicknowledgeonline.com/web/space_sec_session%205_Sreehari%20Rao.pdf

Rajeswari Pillai Rajagopalan and Narayan Prasad Nagendra, "Creation of a Defence Space Agency: A New Chapter in Exploring India's Space Security, February 23, 2017, available at http://www.orfonline.org/expert-speaks/creation-of-a-defence-space-agency-a-new-chapter-in-exploring-indias-space-security/