# Investments in the Space and Cyber Realm for India's National Security

Puneet Bhalla

National security is not restricted to securing the land, air and maritime boundaries and pursuing strategic interests but encompasses all aspects that have a bearing on the nation's well-being. Outer space and cyber space have emerged as the new enablers for nations, enhancing the speed and efficiency of national security and socio-economic efforts and also in providing novel applications for the same. In an information dominated world, they are instrumental in providing the competitive edge among the global community, strategic and tactical superiority in conflict situations, and projection of national power and influence. In addition to capability enhancement towards national aspirations, investments are also necessary for securing these facilities against deliberate or unintentional intrusions or attacks and in ensuring safe and sustainable operations. As the resources available to the nation are not infinite, their utilisation would need to be optimised.

## Outer Space

Space-enabled services enhance existing technological capabilities or create novel applications to support national security objectives – both military and non-military. They have maintained their pivotal role towards strategic

Group Captain **Puneet Bhalla** is former Senior Fellow, Centre for Land Warfare Studies, New Delhi.

**N.B.** The views expressed in this article are those of the author in his personal capacity and do not carry any official endorsement.

**Outer space and cyber space have emerged as the new enablers for nations, enhancing the speed and efficiency of national security and socio-economic efforts and also in providing novel applications for the same.**

security even as their employment for force enhancement functions in support of military operations has continued to grow with improving capabilities and performance. At the same time, these services have become integral to activities aimed at a nation's economic and societal development. With growing participation, commercialisation has become an integral part of space operations and is receiving active governmental support. Towards strategic and tactical missions, space systems provide Intelligence, Surveillance, and Reconnaissance (ISR), global communications, meteorological inputs, early warning of missile launches and environmental monitoring. These contribute towards a more efficient Command, Control, Communications, Computers, Intelligence, Information, Surveillance, and Reconnaissance (C4I2SR) network, enabling an informational advantage, speeding up of the decisional cycle and greatly enhancing the combat potential. Positioning, Navigation, and Timing (PNT) services, available through global navigation space systems such as the Global Positioning System (GPS), empower the militaries in conventional missions through well coordinated and synchronised operations and precision weapon guidance and targeting. An important facet has been remote control of platforms like the Unmanned Aerial Vehicle/ Unmanned Combat Aerial Vehicle (UAV/UCAVs) at large geographical distances. Space-based capabilities are instrumental in space support functions, improving the efficiency of logistics and sustainment missions, thereby ensuring freedom of action, extending the reach of operational forces and prolonging their endurance.

Militaries 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 and all force modernisation efforts are also centred on them. Space is going to be of increasing importance as the emphasis continues to shift from platform-centric warfare to network-centric warfare.

**Space-based capabilities are instrumental in space support functions, improving the efficiency of logistics and sustainment missions, thereby ensuring freedom of action, extending the reach of operational forces and prolonging their endurance.**

Space has also become an enabler for many critical civilian applications. Remote sensing data is being utilised extensively for governance, socio-economic programmes, ensuring food and water security, monitoring and management of natural resources and the environment, mitigating and managing disasters, and so on. Satellite communications support several critical economic functions that require quick and efficient information sharing among dispersed stations. They also allow connecting to remote areas of the country. Banking and financial services, oil and gas industry, health and education and Direct to Home television are among the areas where satellite communication has found effective application. PNT services are finding increasing use for critical infrastructure applications in various sectors such as transportation, financial services, electric transmission, supply chain management and mobile telephony.

**Vulnerabilities**: While space operations have always been vulnerable to natural interferences, progressive developments in the domain have also resulted in the emergence of unique novel challenges to space

security and the sustainability of the environment. Greater participation in the domain and commercial prospects has more players vying for the prime orbital slots, the radio frequency spectrum, and a larger share of the market. Overcrowding and increasing space debris is adversely affecting the survivability of satellites. The environment is, thus, becoming more contested, congested and competitive with the consequent increase in the potential for disruption of operations.

Space is being used extensively by the advanced space-faring nations for supporting military operations and most new entrants would also leverage their access for these purposes. A corollary to this is that all assets in space providing a strategic or military advantage can be designated as valid targets in case of hostilities. Consequently, the advanced nations are making efforts to dominate and control the environment to protect their interests and assured access to the realm and the less capable ones would do the same to gain an asymmetric advantage through degradation and destruction of systems. Both these strategies demand development of counter-space capabilities that would include offensive capabilities, as well as those aimed at system negation. These would not just target the space segment but also the ground based infrastructure and the Telemetry, Tracking, and Control (TT&C) network. The US, Russia and China have demonstrated Anti-Satellite (ASAT) capabilities – both soft kill and hard kill options –and continue to pursue such programmes. Additionally, most of the technologies being developed for peaceful applications in the domain have an inherent ASAT potential. Such capabilities in the hands of rogue nations or non-state actors, who have limited interests in the domain, could be extremely dangerous.

In India, 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. In recent years, national security challenges have necessitated a tacit acceptance of the use of the domain

for meeting national security objectives. In July 2013, the Geostationary Satellite (GSAT)-7 was launched for the dedicated use by the Indian Navy for supporting its network-centric operations. The GSAT-6, launched in August 2015, also supports military applications. The Indian Regional Navigation Satellite System (IRNSS) constellation has been deployed with national security objectives in mind. The requirement, however, is of a comprehensive plan aimed not only at capability-building but also at securing our interests in the domain.

In India, vast and inhospitable land borders with inimical neighbours and an equally long coastline need to be secured through advanced measures. Energy security has necessitated expansion of the area of interest from the Gulf of Aden to the Strait of Malacca. The presence of nuclear tipped missiles in the neighbourhood dictates an efficient early warning network for Ballistic Missile Defence (BMD). Internal security challenges continue to affect some parts of the mainland. With its growing regional stature, employment of the armed forces to meet Out of Area Contingencies (OOAC) cannot be ruled out. Addressing such vast and diverse challenges cannot be achieved without abundant space-enabled capabilities.

To meet the futuristic challenges, the armed forces have already been investing in platforms and technologies that are heavily dependent on space for their effectiveness. These services would also be key enablers in all future operations in a networked environment. As China makes rapid progress in its space programme, it is important to develop comparable capability to offset the advantages that the domain could afford to its military. Meanwhile, many of the technology dependent services promoting national growth have also been increasing their use of space-driven services. On the other hand, budgetary allocations for the sector, which currently are at 0.07 percent of the Gross Domestic Product (GDP), are unlikely to change much in the near future. The requirement, therefore, is of a pragmatic national effort that dictates optimal utilisation of the resources and seeks solutions outside the conventional boundaries.

Major current challenges pertain to both capability and capacity to meet the requirements of diverse users. The armed forces desire an increase in the revisit times of the satellites, a wider regional coverage area and more multi-spectral imagery. Facing two adversaries with advanced military and missile technologies, the capability for Electronic Intelligence (ELINT) and early warning satellites is a necessity. There is also a shortage of indigenous transponders to meet the nation's burgeoning requirements, resulting in heavy dependence on foreign satellites. Besides the outflow of valuable foreign exchange, this also adversely affects the strategic interests. ISRO's capacities for both satellite building and launch have been found inadequate to cater to national and commercial requirements. While the GPS Aided GEO Augmented Navigation (GAGAN) and IRNSS constellations have been deployed, their employability has been hindered because of issues related to user terminals. Technology and capability deficits can be addressed both through the traditional incremental development approach and by embracing revolutionary emerging technologies and applications. Futuristic technologies like micro-technology, nano-technology, additive printing (3D printing), robotics and artificial intelligence have multi-discipline relevance and should be developed as a national effort. The nation's technological prowess can best be harnessed by incentivising and involving the private sector and academia in the Research and Development (R&D) efforts. Self-reliance would reduce the costly procurements of components from foreign vendors, provide the much needed strategic independence and make these systems much less prone to cyber attacks or espionage.

The most radical technological application in the sector is that of the smaller satellite – mainly the CubeSat form factor – that provides advantages in terms of lower cost, weight reduction and shorter development time. Defining and adoption of the CubeSat standard has allowed flexibility in the designing and deployment of these satellites. The steady improvement in their performance has further led to exploration

of revolutionary applications such as constellations and Distributed Space Systems (Swarms), which can further enhance the capabilities through synergising. Constellations can cover large swaths and enable multi-spectral coverage and better temporal resolution, while the larger numbers provide redundancy. Their employment for ELINT missions has already been proven. These applications are being explored to complement larger satellites' missions and are expected to replace them in the future. ISRO needs to let go of its initial hesitation and pursue this technology to provide cheaper alternatives for capacity building. The agency's recent efforts at pursuing futuristic technologies like electric propulsion and high throughput satellites towards capacity enhancement are noteworthy.

**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.**

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.[1] 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.[2] Additionally, technologies matured for the ballistic missile programme could be explored for developing dedicated launch capability for microsatellites. Such a capability could also be utilised to develop launch on demand capability to meet operational needs, augment constellations or replace damaged satellites at short notice. This, along with responsive modular satellites and responsive buses and payloads, would enable operationally responsive systems.

The traditional compartmentalised way of working has resulted in overlooking of converging interests and a demand for captive capacity by all. This can be overcome through coordinated planning among various space dependent sectors, wherein prioritisation and consolidation of national requirements would eliminate duplication of effort and maximise the use of limited resources. The resultant space architecture would be more coherent and take advantage of synergies to be more cost-effective and efficient. This would also encourage joint technology development. A similar approach is recommended towards a holistic space capability roadmap for the armed forces that supports the complete range of military operations. Dual-use platforms need to be explored wherever possible. Besides the cost benefits, such an approach would help conceal military capacities and also provide redundancy through dispersed capabilities.

An identical methodology needs to be employed with respect to efficient downstream utilisation of sensor data through integrated national and military Geographical Information Systems (GIS). This would rationalise the demands and provide more time relevant data to the end user. Effort from indigenous industry is needed towards developing compatible sophisticated end user terminals in sufficient numbers. Space operations are already being supported by almost 500 Indian small and medium scale enterprises, which are nurtured by the agency through technology transfer, funding and hand-holding. A National Space Law is also under consideration and, when enacted, it is expected to further energise the space industrial base and encourage private investment in space R&D. 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. An indigenous consortium would also be more conducive to accommodating national security requirements.

To overcome the limitations related to ISRO's civilian mandate, a parallel organisation needs to be created to cater to dedicated military requirements, including the launch on demand capability. A Defence Space Agency would optimise resource utilisation and be a common interface for planning and executing military programmes. As reliance on satellites increases, the domain becomes more stressed and regional adversaries acquire ASAT capabilities, there is a need to invest in ensuring continued availability of these services. 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 Space Situational Awareness (SSA) capability is highly inadequate for space security functions. The data derived from other such networks, which is available through the public domain, is not accurate enough. There is a necessity to gradually develop SSA capability by building terrestrial radar and optical sensors and the supporting computing and analytical ground infrastructure. Simultaneously, India must enter into data sharing agreements with countries with better capabilities.

**Current Indian Space Situational Awareness capability is highly inadequate for space security functions. The data derived from other such networks, which is available through the public domain, is not accurate enough.**

The obligation of synergistic national efforts would be best served by devising a comprehensive National Space Policy, which would define the national process for developing and harnessing space capabilities, including coordinated R&D. It would enable greater coherence of action, more rational resource allocation and act as an international Confidence-Building Measure (CBM). A classified National Space Security Policy could be a sub-set,

**The armed forces should evaluate creating a cadre of space professionals, skilled in exploiting these capabilities in support of diverse operational functions. These specialists would more effectively contribute to system design and development, formulation of long-term development and procurement plans and devising of doctrines and strategies.**

identifying the potential strategies and plans and the institutional framework to counter the threats. The envisaged increase in space operations would need to be supported through appropriate human resource development – enhancing the strength of skilled manpower and spreading awareness among decision-makers and end users. The armed forces should evaluate creating a cadre of space professionals, skilled in exploiting these capabilities in support of diverse operational functions. These specialists would more effectively contribute to system design and development, formulation of long-term development and procurement plans and devising of doctrines and strategies. These efforts would benefit through inter-departmental postings of domain experts and technologists.

## Cyber Space

Cyber space is a man-made domain consisting of the interconnected networks of computing machines and communication devices and the information contained on these networks. Advancements in the cyber domain have not required a protracted thrust by governments at capability building as the transformational nature of the technology, its commercial potential and cheaper access has caused a self-sustaining expansion of capabilities and capacities. The increasing dependence on the networks, however, has resulted in a surge in the number and sophistication of cyber attacks that exploit the hardware or software vulnerabilities of the networks with diverse motivations and consequences. Consequently, a greater share

of cyber capability development by governments and organisations today is centred on cyber security – securing the networks against unintentional or unauthorised access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information.[3]

Cyber intrusions could target the government agencies and departments, private corporations or individuals, with diverse impacts on national security. These could be undertaken for espionage, to commit cyber crime or for denying or disrupting critical national infrastructure systems like power grids, telecommunications networks, transportation systems or services like the water services or the financial and banking operations. They could be used for social engineering – spreading disinformation and moulding public opinion with an intention to destabilise the internal security environment of the country. As network centricity becomes integral to military operations, military equipment and operations could be assaulted to gain strategic or tactical advantage. These attacks could even be used to cause kinetic effects, acts of sabotage or to hamper national response mechanisms, all of which would endanger lives. More widespread and systematic attacks could escalate tensions among states.

The perpetrators of these attacks could be anyone from an individual to hacking syndicates that work independently or are covertly supported by governments and corporations. States as well as non-state actors could seek an asymmetric advantage by employing such attacks to undermine an adversary's security and stability. Elementary players would aim to exploit existing vulnerabilities, the more proficient ones would identify the hidden vulnerabilities and the highly skilled, well resourced ones would patiently develop tools and techniques to inflict vulnerabilities in the systems. With greater technological capability, the nature and scale of cyber attacks has continued to evolve. They are now more targeted and decisive, with clear political, economic or military motivations

**Cyber situational awareness, the ability to monitor the domain, identify the vulnerabilities and detect the intrusions is still not sufficiently developed.**

and intentions. The traditional lines that would earlier help distinguish between the types of attacks and the motivation of their perpetrators has blurred. While the state actor could resort to an attack to undermine security or stability, a similar attack could now be undertaken by non-state actors for extortion or for obtaining information that could be sold to third parties.

An increased number of reported cyber security incidents which are becoming ever more potent and aggressive have exposed the vast vulnerabilities of this critical domain. Meanwhile, the networks continue to expand and become more complex and their interdependencies continue to grow, further enhancing the vulnerabilities and increasing the difficulty in providing comprehensive protection. The environment is highly dynamic and preventive and defensive counter-measures and reactive strategies, even with continuous efforts, are finding it difficult to keep pace with the fast evolving threats. Cyber situational awareness, the ability to monitor the domain, identify the vulnerabilities and detect the intrusions is still not sufficiently developed. Attempts at enhancement are hampered by concerns on privacy, freedom of speech, and the free flow of information. Even as detection rates have gone up through concerted efforts, cyber forensics needs to be developed for attribution, as the attacker can hide his track easily in the intricate, borderless domain. International legal regimes have failed to keep pace with the rapid technological advancements in the domain. Advanced nations, whose dependence on space and cyber space exposes them to asymmetric risks of disruption, are responding to these limitations by developing effective deterrence against misadventures, including offensive counter-attack capability. Both the US and China have been actively pursuing establishment of cyber forces, which are expected to have both defensive and offensive capabilities in the domain and many other

nations are following in their footsteps, although more covertly.

India is a growing economy that is investing heavily in computer networks and communication facilities to meet its aspirations. The steadily growing online population has received a further boost with the smart phone revolution, increasing the density and diversity of appliances used for access to the internet. The diversity of machines makes it difficult to put in place comprehensive protection measures. Indian computer machines and networks rely mostly on foreign software and hardware, exposing them to the risks associated with the global information technology supply chain. Most of the data generated in the country is exported and stored in foreign data banks. 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. These would further be added onto by futuristic technological applications such as the Internet of Things (IoT). All these make securing of the domain an arduous task.

**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.**

Unlike in space, the more visible effects and the huge economic losses have spurred the government into being much more responsive to the threat environment in the cyber domain. It has undertaken several steps at protection, detection and containment of these potentially disruptive attacks against the nation's networks. The most significant 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

as the nodal agency for forecasting cyber security threats and incidents and coordinating emergency response actions. It also shares information and issues guidelines, advisories and vulnerability notes relating to information security practices and procedures. These are positive measures but experts have highlighted several shortcomings and loopholes that could affect their efficacy in a more hostile and dynamic environment.

The policy has been criticised for involving multiple agencies and departments in cyber security management without clearly defining the command and control structure or the coordination mechanism. Overlapping responsibilities could lead to decision ambiguities and duplication of efforts, and dilutes accountability. It is ambiguous on the military aspects and the role of the armed forces. There are not sufficient provisions to make it binding or enforceable or to make it more alive to the rapid developments that continue to transform the domain. These have resulted in a vast gap between the conceptualisation and implementation. The government has responded to some of the criticism by taking corrective steps, such as the establishment of a 'National Cyber Coordinator' in 2015 and an ongoing process to form a National Cyber Coordination Centre (NCCC) with an investment of nearly Rs 800 crore. The NCCC is expected to coordinate intelligence gathering and sharing between agencies and even be instrumental in coordinating quick and decisive remediation action. However, such piecemeal, compartmentalised efforts at prevention and response might not bring the desired results.

There is a need to build on the existing foundation and invest in an effective cyber security initiative by focussing on technologies, processes and people.

- Technological and process solutions are required towards eliminating the vulnerabilities of existing networks and improving resilience. Greater indigenisation of hardware would reduce the risks related to global supply chain vulnerabilities. A similar effort in software development and updating and data handling systems would be

beneficial in securing information. Technological protection, prevention and response counter-measures are required to fight all kinds of cyber intrusions, including those related to emerging technologies and their applications. Automated safeguards and scanning, detection and response processes need to be more widely implemented to mitigate risks. Expertise should be employed towards active defence strategies involving predictive analysis – utilising digital trail exploitation, Cloud Computing and Big Data Analytics for continuous threat profiling, predicting the origin and type of attack, and forecasting the nature and direction of future threats. Needless to say this would require the necessary investment in R&D efforts.

**Expertise should be employed towards active defence strategies involving predictive analysis – utilising digital trail exploitation, Cloud Computing and Big Data Analytics for continuous threat profiling, predicting the origin and type of attack, and forecasting the nature and direction of future threats.**

- Achievement of national cyber security objectives would require a coherent and comprehensive national cyber security strategy. The overarching document should also lay down the capability development plan as also the integrated implementation process which would clearly enunciate the tasks and responsibilities, prioritisation of resources, the desired timelines and accountability. The organisational structure should be restructured to define a single apex agency that would control and coordinate all cyber functions and facilitate synergy among various governmental, non-governmental and private bodies at policy and operational levels towards greater functionality and coordinated response. Such a document should be reviewed periodically to respond to emerging cyber security issues and

threats. "Appropriate cyber security legislation would help address information sharing concerns and also define baseline standards to be followed for critical infrastructures.

- People form a critical element of cyber space. There is a need to spread awareness among users, educate decision-makers and provide adequate skill training to cyber professionals. The pool of specialists needs to be enhanced in terms of both quantity and quality to meet future challenges.
- The private sector has been a key developer of cyber technologies and has experience in managing its own networks. Therefore, private companies could contribute to the national security practices by sharing their technological capabilities and best practices. The setting up of the Joint Working Group on Public Private Partnerships in Cyber Security in 2012 by the government was recognition of this potential and these efforts need to be pursued actively.
- Information sharing among all relevant governmental agencies and with the private sector is a must to eliminate system vulnerabilities and reduce and mitigate risks and respond to cyber incidents. This should be supported by appropriate legal and policy safeguards.

Space and cyber, both technologically intensive domains, need to be harnessed optimally for national security. Formulation and articulation of an all encompassing national security policy would help define domain specific strategies and roadmaps. It would also enable re-conceptualisation of organisations and structures for more proportionate representation of domain experts who would better harness the technological potential. Although India has been a strong proponent of peaceful application of technology, it must acknowledge the militarisation of the domains since they have become integral to the nation's security architecture and require investments in military capabilities. Establishment of lateral military organisations such as the Defence Space Agency and Defence

Cyber Agency would enable harmonising capability development among the services, control and coordinate joint assets and ensure synergised operations. They would also enable formulation of joint concepts and doctrines, conduct of integrated training and optimise procurements.

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 and the mutual distrust among nations and the unpredictability of non-state actors is thwarting any 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.

International collaboration with nations with congruent interests should be enhanced for capability and technology development, sustenance of operations and enhancing collective security capabilities. At the same time, India should also be active in important global forums highlighting the global implications of destabilising incidents in the domains and continue its efforts at promoting safety, stability, and security.

## Notes

1. Madhumathi DS, "Space Parks to Lift ISRO Run Rate", *The Hindu*, January 11, 2016, available at http://www.thehindu.com/news/national/isro-conceives-two-space-parks/article8089731.ece
2. Reply to Rajya Sabha Unstarred Question No. 1730, March 12, 2015, "Setting Up Of New Launch Pads", available at http://dos.gov.in/sites/default/files/RU%201730.pdf
3. "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada", A 2010 document, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf