NATIONAL SECURITY AND ITS IMPLICATIONS FOR INDIA AND THE ROAD AHEAD

Dr. Anupma Tomar

Post- Doctoral Fellow, Department of Defence Studies, Meerut College, Meerut

Prof. Mohd Rizwan

Department of Defence Studies, Meerut College Meerut

National security is a concept that a government, alongwith its parliaments, should protect the state and its citizens against all kinds of "national" crises. A national security doctrine helps the statesmen identify and prioritize the country's geopolitical interests. It encompasses the totality of the country's military, diplomatic, economic and social policies that will protect and promote the country's national security interests.

The concept of national security remains ambiguous, having evolved from simpler definitions which emphasized freedom from military threat and from political coercion. Among the many definitions proposed to date are the following, which show how the concept has evolved to encompass non-military concerns:

- "A nation has security when it does not have to sacrifice its legitimate interests to avoid war, and is able, if challenged, to maintain them by war."
- "The distinctive meaning of national security means freedom from foreign dictation."
- "National security objectively means the absence of threats to acquired values and subjectively, the absence of fear that such values will be attacked."
- "National security then is the ability to preserve the nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to preserve its nature, institution, and governance from disruption from outside; and to control its borders."

- "National security... is best described as a capacity to control those domestic and foreign conditions that the public opinion of a given community believes necessary to enjoy its own self-determination or autonomy, prosperity, and wellbeing."
- "National security is an appropriate and aggressive blend of political resilience and maturity, human resources, economic structure and capacity, technological competence, industrial base and availability of natural resources and finally the military might."
- "National security is the measurable state of the capability of a nation to overcome the multi-dimensional threats to the apparent well-being of its people and its survival as a nation-state at any given time, by balancing all instruments of state policy through governance... and is extendable to global security by variables external to it."
- "National and international security may be understood as shared freedom from fear and want, and the freedom to live in dignity. It implies social and ecological health rather than the absence of risk... and is a common right."

The Need for National Security

A country's national security policy is determined by many factors, including external threats, geography, political culture, military capabilities, economic needs, elite opinion, popular opinion (in democracies), and its leaders' perceptions of the country's interests. This conceptual framework manifests itself as foreign policy or national security 'doctrine', which in turn guides leaders in conducting the foreign policy of a country. A national security doctrine helps the statesmen identify and prioritize that country's geopolitical interests. India does not have any such 'doctrine'

Why do we need a National Security Doctrine?

- India has seen crisis after crisis resulting from militancy, insurgency, terrorist attacks, unsettled border disputes, etc. For Ex, Terrorist attack on Pathankot airbase (2016), 26/11 Mumbai blasts, Church Street bomb blasts in Bangalore (2015), border disputes with China, Pakistan, Insurgency in the Northeast, etc. The list goes on and on.
- The Pathankot debacle has triggered a serious debate on the need for a National Security Doctrine.
- There is opacity in the functioning of Intelligence agencies. For Ex, no credible external audit happens, No cohesive command and control structure.
- To fill the gaps in India's security policy planning

- Porous international boundaries, growing terror threats, increasing insurgency within country demand government to envisage and formulate a National Security Doctrine for India.
- The existence of such a document will dissuade adventurism and will reassure our citizens that appropriate measures are in place to protect us.
- Many of India's national security inadequacies stem from the absence of a national security/defence vision.
- It will not only become the basis for strategy-formulation, contingency-planning and evolution of SOPs, but also send a reassuring message to our public.
- It is necessary in the face of having nuclear-armed neighbours, Pakistan and China.
- To define India's role in the world and its commitment to protecting the life, liberty and interests of its people.
- The country should have an overall national security document from which the various agencies and the arms of the armed forces draw their mandate and create their own respective and joint doctrines which would then translate into operational doctrines for tactical engagement.
- In the absence of this, as is the case in India today, national strategy is broadly a function of ad-hocism and personal preferences.

Classification of Threat:

Kautilya wrote in Arthashastra that a state can be at risk from four kinds of threats:

- Internal
- External
- Internally aided external
- Externally aided internal

India's security threat perceptions are a mix of all four shades of threats defined above.

The changing external environment also impacts our internal security. Events in Sri Lanka, Pakistan, Bangladesh, Nepal and Myanmar have direct or indirect linkages with our internal security. Therefore, it can be said that in today's information and digital age, security threats, both internal and external, are inter-related and cannot be seen in isolation from each other.

Over the years, the challenges to our internal security have grown manifold and assumed alarming proportions. Internal security problems have started affecting our country's

growth and development. This is now one of the prime concerns in the top echelons of the Government.

National security doctrine should include the following key elements:

- Political
- Socio-economic
- Governance
- Police & Security Forces
- Centre-State Coordination
- Intelligence
- Border Management
- Cyber Security

1. Political:

First, we need to know the nature of the challenge to our security. It could be secessionist, separatist or even regional in nature. We have to analyse the causative factors of various types of movements and see whether the demands are within the constitutional framework or not.

As a matter of principle, we have to deal the secessionist movements with a heavy hand. Separatist elements have to be kept at a distance. We need a clear policy with stringent laws to deal with such elements. On the other hand, regional aspirations and ethnic demands require reasonably softer and sympathetic approach.

2. Socio Economic:

Socio-economic factors are also at the back of many movements which are big threats to the internal security of the country. Many a times, there are genuine socio-economic grievances of a section of the society arising from acute poverty, unemployment and displacement. In such cases, our approach has to be different.

We need to analyse the factors causing the socio-economic grievances and address all the connected issues. Equitable growth and development is the spirit of our Constitution. Therefore, we have to ensure that development reaches all sections of the society and there are no regional disparities.

3. Governance:

Lack of good governance also provides a tool in the hands of anti-establishment elements, who pose a challenge to the security of the country. Such elements take advantage of

mismanagement and corruption in government schemes, poor implementation of laws and absence of government machinery in the remote areas.

Governance on all fronts becomes an issue whether it is civil administration or policing of the area or the whole of criminal justice system. It is the duty of the state to control all the malaise in governance and provide good governance to the remotest of the areas and control corruption. Otherwise, development of remote areas will be nearly impossible.

4. Police and Security Forces:

It has been seen that, at times allegations of police atrocities and police indifference towards people's problems, aggravate internal security problems. We have seen many a times that agitations are directed against the police or the security forces. Demand for removal of AFSPA is one such example. Police needs to be sensitized so that it becomes people friendly.

We need to carry out police reforms so that the police is seen as a neutral, transparent and professional body. Other security forces aiding state police also need to increase their understanding of the local situation and maintain highest order of efficiency. They need to coordinate with the state police and help achieve overall goal of maintaining the internal security.

5. Centre-State Coordination:

Lack of center-state coordination also leads to many problems related to internal security. This coordination problem exists in all areas from intelligence to operations. We need to develop an institutional framework which resolves all these center-state coordination problems and ensures synergy at all levels.

6. Intelligence:

Intelligence is a major component of Security. We need to be alert against external as well as internal enemies posing a threat to the internal security of the country. Most of the big operations have the back up support of intelligence.

We need to have defensive as well as offensive intelligence to forewarn, neutralize the impending threats and take proactive steps wherever required. We also need to have regular institutional framework to compile, collate and act on intelligence received from various agencies. Multi-Agency Centre (MAC) has made a good beginning in this direction.

7. Border Management:

The country has land borders with seven countries (practically six due to PoK issue) stretching nearly 15,000 kms. We have had wars on three sides of our land borders with

China, Pakistan and East Pakistan (presently Bangladesh). We also had infiltration problems through Punjab and Kashmir borders, illegal immigration problems through Bangladesh and smuggling of weapons through Indo-Myanmar border.

Kashmiri militants have been taking shelter in PoK while North-East extremists are taking shelter in Bangladesh, Bhutan and Myanmar. Therefore, we need to guard our land borders effectively to prevent infiltration by terrorists, illegal immigration, smuggling of weapons and drugs etc. Coastal security also needs special attention and we need to ensure that the roles of Navy, Coast Guard and Coastal Police are clearly defined and all of them work in harmony with each other.

8. Cyber Security:

The Snowden revelations (WikiLeaks) of 2013 have made it evident that future wars will not be traditional wars which are fought on land, water and air. In fact, it appears that cyber space will be the theatre of warfare in the 21st Century.

Therefore, any solid doctrine on security needs to cover this front also. India has just made a beginning in this direction. We need to cover a lot of distance before we could say that we have a safe cyber space.

Attributes of Security:

The main attributes of security are:

i. Secure territorial integrity and protect internal sovereignty

ii. Maintain domestic peace

iii. Prevalence of law and order

iv. Rule of law and equality before law—law of the land should protect everyone irrespective of status

v. Absence of fear from the feared implying individual freedom for people as guaranteed by the Constitution

vi. Peaceful co-existence and communal harmony

Factors Responsible for Security Problems:

There are various reasons, both historical and non-historical, which cause problems for ourinternal security.

However, a few root causes are mentioned below:

i. Unfriendly neighbours

ii. Poverty

iii. Unemployment

iv. Inequitable growth

v. Widening gap between haves and have nots

vi. Failure on administrative front or Governance deficit

vii. Increasing communal divide

viii.. Increasing caste awareness and caste tensions

ix. Rise of contentious politics based on sectarian, ethnic, linguistic or other divisive criteria

x. Porous borders having very tough terrain

xi. Poor criminal justice system and large scale corruption leading to nexus between criminals, police and politicians with the result that organised crime goes on unabated.

We inherited the first three factors at the time of independence. We have failed to resolve all the three issues. Unfortunately, we have added more factors which have multiplied our internal security problems. The fourth, fifth and sixth factors in the above list can be termed as administrative failures and the seventh, eighth and ninth could be due to the rise of partisan politics.

The last two can be attributed to a pronounced deficit of governance. Every problem gets highlighted because of these factors and hostile neighbours leave no opportunity to exploit internal conditions for the pursuit of their own agenda. The declared policy of Pakistan's ISI 'to bleed India through a thousand cuts' proves the point.

Major Challenges to Security:

Independence for India came with some inherited problems related to internal security. The issue of the accession of the state of Jammu and Kashmir to India also came with its own set of problems related to our internal security. The division of the pre-independence India into two nations resulted in large scale unforeseen violence that claimed millions of lives. Thus was born the menace of communalism which was visible again and again in various riots thereafter.

As an emerging nation, we hoped to overcome these problems and embark upon a path of national reconstruction and consolidation, but progress has been hampered by various challenges to internal security faced by the country.

Over the years, India's security problems have multiplied due to linguistic riots, inter-state disputes, caste and ethnic tensions, etc. In 1956, the country was forced to redefine its inter-state boundaries due to linguistic riots.

The 1950s also saw the North-east going up in flames, when in 1954 Phizo raised the banner of revolt in Nagaland and the fire spread to Mizoram, Manipur and Tripura.

The later part of the sixties saw the rise of Naxalism. At the time of independence, India was an under-developed country and had taken up the task of rebuilding the country. The country adopted the equitable and inclusive growth model for growth and development. But, over the years, it has become evident that we have failed on many counts and poverty, unemployment and under-development prevail in the interior regions of the country.

This situation was exploited by various people to pose a very dangerous challenge to the country's internal security in the form of Maoism/Naxalism /Left-Wing Extremism. In 2006, the then Prime Minister even admitted that this was perhaps the biggest challenge to the country's internal security.

The eighties witnessed the growth of the terrorist movement in Punjab, aided and abetted by a hostile neighbour. The nineties saw the beginning of militancy in Kashmir which has slowly become a pan-India phenomena with the onslaught of international terrorism in the hinterland during the past decade.

The rise of Indian Mujahideen (IM) has been another dangerous phenomena in the last decade. This has again been supported by the unfriendly neighbour as became clearly evident during the 26/11 terror attack in Mumbai. As a result, the Centre initiated a number of concrete measures to strengthen its anti-terrorism apparatus.

Transnational organised criminals/mafias have given further boost to international terrorism by forging linkages between organised crime and terrorism. Their funding and modus operandi has mainly been arms smuggling, drugs trafficking, hawala transactions, money laundering and pumping of fake Indian currency notes (FICN) to different parts of the country.

Cyber security is the latest challenge. We could be the target of a cyber-war which could jeopardise our security as most of our vital installations are now based on cyber systems. Any failure to check cyber-attacks could be fatal to our economy and security. The Snowden revelations (Wikileaks) of 2013 have exposed the extent of espionage that is possible through cyber networks.

The phenomenal growth of the internet and mobile communication has demonstrated that social media could play a vital role in spreading disinformation and fanning violence. The exodus of Northeast students from the southern states in 2012 and the Muzaffarnagar riots

in 2013 are some examples of the problems being created due to the fast growing communication systems.

Border management is important for containing threats to our internal security. A weak border management can result in infiltration of terrorists and illegal immigrants from various borders and smuggling of contraband items like arms, drugs and counterfeit currency. There has been an increase in hostility against illegal migrants in the North-east. We are yet to find a satisfactory solution, be it political, social or economical, to this problem.

There are also some non-traditional, non-military threats to our security. These include climatic security, diseases and epidemics, energy and water, food issues, resource wars, poverty and economic disparity, etc.

Challenges in implementing a National Security Doctrine:

- There is a skewed national security decision-making structure that is driven more by idealism and altruism, rather than by realpolitik imperatives.
- National security has suffered neglect for decades due to pre-occupation of our politicians with electoral politics.
- Defining national interests in a multi-party democracy like India that has representation across the ideological spectrum has been hard to achieve.
- Decisions of national security are taken in individual silos rather than cross-domain exchange as subjects are inter-related.
- There is opacity in the functioning of Intelligence agencies for instance there is no credible external audit that happens.
- The agencies that are to provide security cover and neutralise terrorist threats do not have a cohesive command and control structure.
- There has been a gap in political pronouncements in our military capabilities — material as well as organisational.

Where can we draw inspiration from?

In the US, each President, on assuming charge, is required by law to make public the National Security Doctrine that his administration intends to follow. For eg, the national security doctrine of the Obama Administration is the integration of diplomatic engagement, domestic economic discipline, and amity among communities at home with military power to bolster America's standing in the world.

How will it look like?

National Security Doctrine + National Security Strategy

National Security Doctrine: It must encompass the totality of this country's military, diplomatic, economic, and social policies that will protect and promote this country's national security interests.

National Security Strategy: It must include the Command and control structures for meeting eventualities like terror strikes etc. Both the Doctrine and Strategy are interrelated.

- Doctrine: Defines its role in national security. The primary role is to preserve national interests and safeguard sovereignty, territorial integrity, and unity of India against any external threats by deterrence or by waging war. The secondary role is to assist Government agencies to cope with 'proxy war' and other internal threats and provide aid to civil authority when requisitioned for the purpose.

- Strategy: To perform the above role, the Army has a command and control structure with the President of India as the Supreme Commander. Indian Army is controlled by the elected political leadership of the nation (Government of India). Executive control is exercised sequentially through the Union Cabinet, the Defence Minister, and the Chief of Army Staff (COAS). Ministry of Defence handles matters related to personnel, financial, and resource management.

Significance of National Security Doctrine

A National Security doctrine will play a crucial role in security in the following ways:

- This would help in prompt and relevant decision-making as the decisions will be guided by the national security strategy enshrined in the doctrine. This would result in a consistent security response at the time of insurgences.

- It would help in maintaining the proper coordination among security establishments at both Central and State level, and avoid terror attacks which occurred even when intelligence agencies have inputs but due to lack of coordination fail to prevent the attacks.

- This would also make the security establishments more accountable in case of any failure to combat the terror attack.

- Moreover, prompt and successful handling of such attacks would ensure peace, progress, and development in the country.

What purpose will it solve?

Will define India's role in the world and its commitment to protecting the life, liberty, and interests of its people.

Need of the hour:

The immediate requirement is for the Union Government to put together a National Security Doctrine that should have political consensus, publicly transparent, and should reflect the complex challenges facing the country. The doctrine must be accompanied by a national security strategy so that a Pathankot-like situation never happens again.

National security, or national defence, is the security and defence of a sovereign state, including its citizens, economy, and institutions, which is regarded as a duty of government. Originally conceived as protection against military attack, national security is widely understood to include also non-military dimensions, including the security from terrorism, minimization of crime, economic security, energy security, environmental security, food security, and cyber-security. Similarly, national security risks include, in addition to the actions of other nation states, action by violent non-state actors, by narcotic cartels, and by multinational corporations, and also the effects of natural disasters.

Governments rely on a range of measures, including political, economic, and military power, as well as diplomacy, to safeguard the security of a nation state. They may also act to build the conditions of security regionally and internationally by reducing transnational causes of insecurity, such as climate change, economic inequality, political exclusion, and nuclear proliferation.

Potential causes of national insecurity include actions by other states (e.g. military or cyber attack), violent non-state actors (e.g. terrorist attack), organised criminal groups such as narcotic cartels, and also the effects of natural disasters (e.g. flooding, earthquakes). Systemic drivers of insecurity, which may be transnational, include climate change, economic inequality and marginalisation, political exclusion, and nuclear proliferation.

In view of the wide range of risks, the security of a nation state has several dimensions, including economic security, energy security, physical security, environmental security, food security, border security, and cyber security. These dimensions correlate closely with elements of national power.

Increasingly, governments organise their security policies into a national security strategy (NSS); as of 2017, Spain, Sweden, the United Kingdom, and the United States are among the states to have done so.Some states also appoint a National Security Council and/or a National Security Advisor which is an executive government agency, it feeds the head of the state on topics concerning national security and strategic interest. The national security council/advisor

strategies long term, short term, contingency national security plans. India holds one such system in current, which was established on 19 November 1998.

Although states differ in their approach, with some beginning to prioritise non-military action to tackle systemic drivers of insecurity, various forms of coercive power predominate, particularly Military Capabilities.[8] The scope of these capabilities has developed. Traditionally, military capabilities were mainly land- or sea-based, and in smaller countries, they still are. Elsewhere, the domains of potential warfare now include the air, space, cyberspace, and psychological operations.[15] Military capabilities designed for these domains may be used for national security, or equally for offensive purposes, for example to conquer and annex territory and resources.

Consistency of approach

The dimensions of national security outlined above are frequently in tension with one another. For example:

- The high cost of maintaining large military forces can place a burden on the economic security of a nation And annual defence spending as percent of GDP varies significantly by country. Conversely, economic constraints can limit the scale of expenditure on military capabilities.

- Unilateral security action by states can undermine political security at an international level if it erodes the rule of law and undermines the authority of international institutions. The invasion of Iraq in 2003 and the annexation of Crimea in 2014 have been cited as examples.

- The pursuit of economic security in competition with other nation states can undermine the ecological security of all when the impact includes widespread topsoil erosion, biodiversity loss, and climate change.[35] Conversely, expenditure on mitigating or adapting to ecological change places a burden on the national economy.

If tensions such as these are mismanaged, national security policies and actions may be ineffective or counterproductive.

Cyber is often touted as the fifth dimension of warfare — in addition to land, sea, air and space. It increasingly appears that the cyber warfare is going to become a regular part of the arsenal of nations

As far as India is concerned, it ranks 3rd in terms of the highest number of internet users in the world after the USA and China, but still, its cybersecurity architecture is in a nascent approach.

The changing military doctrines, all across the world, favour the need to raise cyber commands reflecting a shift in strategies along with building deterrence in cyberspace.

Cyber Warfares and India

- About: It is the use of computer technology to disrupt the activities of a state or organization; deliberately attacking information systems for strategic or military purposes.

  - Cyber warfare typically involves the use of illegal exploitation methods on the internet, corruption or disruption of computer networks and software, hacking, computer forensics and espionage.

- Arguments in Favour of Cyber Warfares: Tempered by responsible use and appropriate controls, cyberwarfare is a safer and more flexible strategic alternative, one critical step between sanctions and bombs.

  - Minimises Human-life Loss: Reducing loss of human lives forms one of the core principles of ethics of war.

    - Cyberwars can be seen as an opportunity to decrease global violence and can shift wars' focus away from human casualties.

  - Prevents Physical Territorial Invasions: Fighting digitally offers a unique opportunity; the continuation of politics by other means, without the physical invasion of a sovereign territory.

- Arguments Against Cyber Warfares:

  - Threat to International Security: Cyber warfare attacks on military infrastructure, government and private communications systems, and financial markets pose a rapidly growing but little understood threat to international security and could become a decisive weapon in future conflicts among States.

  - More Number of Countries to Engage in Wars: Once cybertechnology enters as an important variable in nations' defence policies, the size of a country will cease to matter.

    - Even smaller countries empowered by cybertechnology will be equal to the larger countries like the US, Russia, India or China, in their capability to cause unacceptable damage.

  - Lowering Threshold of Entry into War: Weapons in the 21st century will merely mean a cyber button on the desk of the nation's military/ the leader of the government.

- Geographical land, population, or GDP will be irrelevant in war-making capacity or deterrence.
  o More Frequent Conflicts: With cyber warfares becoming a norm, each nation will have to be more prepared for bilateral conflicts that are based on cyber warfare rather than in multilateral acts of conventional war or rely on military blocs for mobilisation.
- Threats to India:
  o Past Experiences: India has been the victim of cyber attacks multiple times in the past.
    - In 2009, a suspected cyber espionage network dubbed GhostNet was found to be targeting, amongst others, the Tibetan government in exile in India, and many Indian embassies.
    - The power outage in Mumbai in 2020 is also suspected to be the result of an attack by a Chinese state-sponsored group.
  o Threats from China: The real danger to India lies in targeted cyber attacks coming from adversarial nation states.
    - Countries like China can bring immense assets to bear in carrying out sophisticated cyber attacks.
  o Lack of Cyberspace Infrastructure: India is one of the few countries which still does not have a dedicated cyber component in its military.
    - The setting up of a Defence Cyber Agency was announced but came out only as a typical half-hearted step characterising India's lack of strategic planning process.

Way Forward

- Bringing Changes to the National Security Policy:
  o Clarifying the Objectives: The National Security Policy in the 21st century shall define what assets are required to be defended and the identity of opponents who seek to overawe the people of a target nation by unfamiliar moves to cause disorientation of people.
  o Setting Priorities: The national security priorities will require new departments for supporting several frontiers of innovation and technologies; hydrogen fuel cells, desalination of seawater, thorium for nuclear technology, anti-computer viruses, and new immunity-creating medicines.
    - This focus on a new priority will require compulsory science and mathematics education.

- Also, every citizen will have to be made aware of the new remote controlled military technology and be ready for it.
  - o Changing the Strategy: The strategy required for the new national security policy will be to anticipate the enemies in many dimensions and by demonstrative but limited pre-emptive strikes by developing a strategy of deterrence of the enemy.
    - For India, it will be China's cyber capability factor which is the new threat for which it has to devise a new strategy.
  - o New Agenda: The agenda for the new strategy will be to focus on; critical & emerging technologies, connectivity & infrastructure, cyber security and maritime security.

- ▪ Role of Policy Makers: The government should carve out a separate budget for cybersecurity.
  - o Creating a central body of cyber warriors to counter state-sponsored hackers.
    - India's talent base in software development should be harnessed by providing career opportunities.
  - o Bootstrapping the cybersecurity capability programme in states through central funding.

- ▪ Defence, Deterrence and Exploitation: These are the three main components of any national strategy to counter cyber threats.
  - o Critical cyber infrastructure must be defended and individual ministries and private companies must also put procedures in place to honestly report breaches.
  - o Deterrence in cyberspace is a hugely complex issue. Nuclear deterrence is successful because there is clarity on the capability of adversaries but cyber warfare lacks any such clarity.
  - o Exploiting cyberspace to achieve national security objectives. The preparation for this will have to start with the Indian military gathering intelligence, evaluating targets and preparing the specific tools for cyber attacks.

Its major objective is to deter the use and threat of the use of nuclear weapons by any State or entity against India and its forces. Also, India will not be the first to initiate a nuclear strike but will respond with punitive retaliation if deterrence fails. It is confined to only one aspect of India's security framework.

Recommendations

- 5 key areas in draft National Security Policy that Shyam Saran, former chairman of the National Security Advisory Board (NSAB), has prepared and handed over

to the government in January 2015: Domestic security, External security, Military preparedness, Economic security and Ecological security.

- "Strategic communication" is of overarching importance in National Security which must be improved. A command control and communication centre must be built.

- The NSD should guide various doctrines related to external and internal security to fill a huge void in the higher defence management of the country.

- The policy must go much beyond issues of national security and encapsulate the domain of constitutional rights as well.

- It must take an all-inclusive approach to national security integrating diplomatic engagement, domestic economic discipline and amity among communities at home with military power.

- We need to tailor our strategic defence doctrine to create long-term measures towards a deterrent based on severe retribution.

- Emerging strategic technologies like Artificial Intelligence, robotics and miniaturised wars are likely to play an increasingly important role in future warfare, this must be taken care of.

- Developing a National Security Doctrine is as much about the future vision of a country as it is about its past. The need of the hour is to put together a National Security Doctrine that should have political consensus, publicly transparent and should reflect the complex challenges facing the country. The doctrine must be accompanied by a national security strategy.

- Once cybertechnology becomes a key variable in the defence policies of a nation, land size or GDP size are irrelevant. Hence, clearer strategy and greater transparency are the need of the hour to improve India's cybersecurity posture.

- A clear public posture on cyber defence and warfare boosts citizen confidence, helps build trust among allies and clearly signals intent to potential adversaries, thus enabling a more stable and secure cyber ecosystem.

References

Romm, Joseph J. *(1993).* Defining national security: the nonmilitary aspects. *Pew Project on America's Task in a Changed World (Pew Project Series). Council on Foreign Relations. p. 122.* ISBN 978-0-87609-135-7. Retrieved 22 September 2010.

Jump up to:[a][b][c] Paleri, Prabhakaran *(2008).* National Security: Imperatives And Challenges. *New Delhi: Tata McGraw-Hill. p. 521.* ISBN 978-0-07-065686-4. Retrieved 23 September 2010.

Jump up to:[a b c d e f g h i j] Romm, Joseph J. *(1993).* Defining national security: the nonmilitary aspects. *Pew Project on America's Task in a Changed World (Pew Project Series). Council on Foreign Relations. p. 122.* ISBN 978-0-87609-135-7. Retrieved 22 September 2010.

Quoted in Paleri (2008) ibid. Pg 52.

Brown, Harold (1983) Thinking about national security: defense and foreign policy in a dangerous world. As quoted in *Watson, Cynthia Ann (2008).* U.S. national security: a reference handbook. *Contemporary world issues (2 (revised) ed.). ABC-CLIO. pp.* 281. ISBN 978-1-59884-041-4. Retrieved 24 September 2010.

MAIER, CHARLES S. Peace and security for the 1990s. Unpublished paper for the MacArthur Fellowship Program, Social Science Research Council, 12 Jun 1990. As quoted in Romm 1993, p.5

Definition from "Proceedings of Seminar on "A Maritime Strategy for India" (1996). National Defence College, Tees January Marg, New Delhi, India. quoted in Paleri 2008 (ibid).

Jump up to:[a b c d e] *Ammerdown Group (2016).* "Rethinking Security: A discussion paper" (PDF). *rethinkingsecurity.org.uk*. Retrieved 2017-12-17.

Jump up to:[a b c d e] *Rogers, P (2010). Losing control : global security in the twenty-first century (3rd ed.). London: Pluto Press.* ISBN 9780745329376. OCLC 658007519.

"National Security Strategy". *Office of the Security of Defense.*

Jump up to:[a b c d] *Spanish Government (2013).* "The National Security Strategy: Sharing a common project" (PDF). Retrieved 2017-12-17.

Jump up to:[a b c d e] *Sweden, Prime Minister's Office (2017).* "National Security Strategy" (PDF). Retrieved 2017-12-18.

Jump up to:[a b c] *UK, Cabinet Office (2015).* "National Security Strategy and Strategic Defence and Security Review 2015". Retrieved 2017-12-17.

Jump up to:[a b c d e] *US, White House (2015).* "National Security Strategy" (PDF). *Archived from* the original (PDF) *on 2016-10-06.* Retrieved 2017-12-17.

Jump up to:[a b] "War in the fifth domain". *The Economist*. Retrieved 2017-12-18.

South Africa, Department of Defence (2015). "South African Defence Review, 2015" (PDF). *Archived from* the original (PDF) *on 2017-06-09.* Retrieved 2017-12-18.

France (2017). "Strategic Review of Defence and National Security" (PDF). Retrieved 2017-12-18.

Olika, O (2016). "Unpacking Russia's New National Security Strategy". *www.csis.org*. Retrieved 2017-12-18.

"Highways For Travelers". Transportation Security Administration. *Archived from* the original *on 15 September 2012.*

"TSA | Who We Are". *Archived from* the original *on 2008-12-16.* Retrieved 2008-12-07.