Occasional Paper No. 06/2021

India's National Security:
Integrating Idea with the Policy Making

PPF- Centre for Neigbourhood Studies

August 2021

Spreading Awareness **Building Capapcity** **Promoting Resilience**

India's National Security:
Integrating Ideas with Policy Making

Gautam Sen

"***Over the last 40 years, the world has gradually entered into a post-Clausewitzan state where the wars are undeclared, the battlefields can be anywhere, the uniforms are optional, and the combatants as well as the targets are often "civilian". Conventional militaries have repeatedly attempted to utilize technology to meet the new challenges posed, but even the most advanced technology has provided little more than meaningless short-term victories rendered futile in months, if not weeks."***

William S Lind & Greg Thiele, "The View From Olympus: The Fourth Generation Handbook", Castilla House Press, USA, 2015

India's National Security:
Integrating Ideas with Policy Making

PRELUDE

Policy is an outcome of opportunities and resources. What has to be determined is whether the opportunities are existing and the resources are adequate to exploit the opportunities to enunciate a policy for implementation. In a democratic system of governance any policy, confidential or otherwise, falls in the domain of Public Policy nomenclature and its creation must be holistic in nature, incorporate the consensus in amongst the stakeholders. The stakeholders comprise of the representatives of the relevant public sector, the private sector and the public intellectuals at large. The public sector represented by the government which provides the priorities, the rationale and the fiscal and financial outlays by defining the parameters of the policy making within the framework of national interest and political ideology. The private sector must act as a means to achieve the goals by providing the platform for creating a startup in the field of technology and deployment of appropriate manpower. The public intellectuals may belong to the academia or the activists, the advocators, the non-government bodies, the legal experts etc. etc... They work in the abstract area of ideas to work out a framework where they provide a strategy to bridge the gap between the realm of ideas and the domain of public policy making by synergizing the Public and the Private Sectors in an interdependent mode and hence evolve a win-win situation.

The conceptualization of this above model is explicitly and implicitly for incorporation in a democratic form of governance which is transparent in nature, where the spirit of debate and the freedom of speech is taken for granted, and where the elected representatives in the legislature, leaders of the private sector and the public intellectuals can all be synergized in a unified, constructive and ethical ways within the legal framework of the Constitution.

This conceptualization of the above model of policy making is being evolved in this deliberation particularly in the Indian context and specifically in securitizing the Indian national security domain which has experienced a series of catastrophes from within its post independent period in the last century and continuing threats from without in the 21st century and hence have to be formulated in terms of larger goals and aspirations to which this civilizational community of India has committed itself with the objectives of achieving;

1. National stability and integrity
2. Social, political and economic progress
3. Peace and stability in our relations to other states.

NORMATIVE ASPECTS OF INDIA'S NATIONAL SECURITY

The problems related to the formulation of India's national security policy must be seen in terms of the goals enumerated in the preceding section. If this may be called the cultural dimension of the problems of national security, we also have to look at the problems of political perspectives as well. Here we have to consider a complex interaction between our

perceptions of our neighbors beyond the border as well as the larger superpowers and their perceptions and assessment of our situation and our objectives. It is within this matrix of relationship that the specific goals of our national security strategy gets structured. The cultural and political aspects of the problems create a texture of tasks and priorities of decision making and possible options for action.

The actualization of our objectives as modulated and structured requires an adequate process of institutionalization ranging from economic to the administrative and legal preconditions represented by the Public, the Private and the Public Intellectuals to bridge he gap between the realm of ideas and the domain of public policy making. This institutionalization of our national security efforts themselves create further problems and difficulties. Hence all the three dimensions viz. the cultural, socio-political and institutional enter in a complex interaction calling for skills and patterns of leadership at all levels og the problem.

Therefore, we have a final dimension of how various forms of leadership may be required to respond creatively to the complexities of the problem. In this whole endeavor, the role and responsibilities of the public intellectuals to bridge the gap between the realm of ideas and the domain of public policy making is seminal as well as most important. A clear articulation of the various facets of the situation, their complex relationship and a sharp awareness of the possible contributions, tensions and pressures that must be overcome, also particularly the contribution of scholars in the cultural and philosophical disciplines will be needed to examine the normative aspects of the problems of security in light of ideals to which India is committed e.g. non-alignment, national security, social justice and global peace.

It is equally important while discussing the normative aspects of India's national security perspectives, to pay attention to the essay written by K C Bhattacharya entitled "Swaraj in Ideas" in which he cautions every Indian policy maker not to fall in the trap of "slavery of mind", and incorporate any new idea after giving our own ideas equal opportunities to be incorporated. The text of the essay has been placed in ANNEXTURE A. Though written in 1930 which was not published till 1953, its contents are seminal to every aspect of policy making not only in the Indian context but also at the universal global level.

OVERVIEW ON POLICY AS A TERM OF REFERENCE

What is Policy?

There is no simple answer to this question Perhaps that is why so many people claim to have little or no understanding of policy. In fact, many would say that they don't "do policy." Others maintain that it has only minor relevance to their work – or, for that matter, their lives. Not so. We literally eat, drink and breathe public policy. Public policy determines the quality of the air we breathe and the water we drink. It affects the food we eat – how it is harvested, where it is distributed and sold, and how much we pay. It controls the way in which we clean and monitor (or not in the case of the Walkerton tragedy) the safety of the water supply. Public policy sets limits on air emissions – though, of late, governments seem to be issuing warnings of poor air quality more than doing anything significant to clean it up. Transportation is another example of a domain governed by a variety of public policies, most of which are concerned with the safety of travelers. Public policy also regulates the public

airwaves by way of licensing and other rules (the licensing for satellite radio is a hot topic at the moment). It determines the components of Canada's tax regime – which combines income, sales and payroll taxes – and their respective levels. These are only a few examples of how public policy affects us both profoundly and pervasively. It influences virtually every aspect of our lives. This paper discusses the concept of policy from a general perspective. It does not focus upon one specific area or program so much as the key elements embedded in the process of policy development. It is intended to support the work of two comprehensive community initiatives – Vibrant Communities and Action for Neighborhood Change –which are engaged in local efforts to improve the quality of life.1 Vibrant Communities is a national project that links 15 communities seeking effective local solutions to reduce poverty. Action for Neighborhood Change (ANC) is a pan-Canadian project that involves four national and five local partners for the purpose of revitalizing five selected neighborhoods across the country. Both Vibrant Communities and the ANC projects incorporate a policy dialogue, which promotes coordinated management among various federal departments. The policy dialogue also acts as a vehicle for encouraging governments to engage with community participants in discussions of relevant policy, program and administrative issues [Torjman 2005]. There are different ways to look at policy

a. Substantive and administrative policy

Early in these structured policy deliberations, it is clear that there are different kinds of policy. They are:

1. First is concerned with the legislation, programs and practices that govern the substantive aspects of community work. This type of policy covers income security, employment initiatives, child care services and social exclusion.
2. The second type of policy focuses largely upon administrative procedures related to the collection of statistical information on neighborhoods and the evaluation of complex community programs.

b. Vertical and horizontal policy

Substantive and administrative policy can be further classified as vertical or horizontal policy. The former refers to policy that is developed within the organization that has responsibility for its implementation. Vertical policy is what we think of as the normal or traditional way in which policy decisions are made. Vertical policy is developed within a single organizational structure and generally starts with broad overarching policy, sometimes called "corporate" or "framework" policy. Such decisions are made at head office and guide subsequent decisions throughout the organization. At the regional level we might develop regional or "strategic" policy, which translates the national decisions to the regional level, taking into consideration the specific context. Finally, the regional policy is made specific enough to guide operational decision-making [Smith 2003: 11]. Horizontal policy-making, by contrast, is developed by two or more organizations, each of which has the ability or mandate to deal with only one dimension of a given situation. Horizontal or integrated policy is created between parts of an organization or among organizational components that are similar in hierarchical position [Smith 2003: 11-12]. Governments increasingly are focusing their efforts upon horizontal policy-making in recognition of the fact that many of the objectives they seek to achieve are complex and relate to the mandates of two or more departments, jurisdictions or non-governmental organizations. Areas of common interest include, for example, climate change, Aboriginal issues and the range of concerns rooted in cities and

communities. Collaborative arrangements are being driven partly by the pressure to enhance performance and achieve measurable improvements in service delivery. The 2005 Budget was the latest in a string of federal documents that highlight the need to strengthen and modernize public sector management. Horizontal management is seen as one way to ensure that the federal government acts as a vibrant, cohesive and coherent national institution [Fitzpatrick 2000].

c. Reactive and proactive policy

Policy can also be categorized as reactive or proactive. Reactive policy emerges in response to a concern or crisis that must be addressed – health emergencies and environmental disasters are two examples. Proactive policies, by contrast, are introduced and pursued through deliberate choice. The national skills and learning agenda exemplifies this approach. Knowledge and learning increasingly have been recognized as vital keys that unlock the doors to both economic wealth and social well-being. In recognition of these crucial levers, the federal government launched in February 2002 two separate, but linked, national strategies: the National Strategy on Innovation and the National Strategy on Skills and Learning. Together, these strategies sought to ensure that Canada has the most skilled and talented labour force in the world. This intent was reinforced in the fall 2002 Speech from the Throne which profiled Canada as "a world leader in innovation and learning, a magnet for talent and investment." The 2003 federal Budget built on this theme by announcing Ottawa's commitment to "provide new opportunities to learn and to work for all Canadians."

d. Current and future policy

Finally, there is yet another way to categorize various policies: those that are currently on the public agenda and those that are not [Smith 2003: 10]. Issues already on the public policy agenda (e.g., health care) often have high profile. A formal process to amend or improve the existing arrangement generally is in place. If an issue is not currently or never has been 'alive' on the public agenda, then there is work to be done in making the case for its importance and raising awareness about the implications of non-response. Making the case usually involves gathering evidence that supports the policy. Relevant evidence includes, for example, research findings, evaluation data and results from focus groups. (While the federal government actively promotes the concept of 'evidence-based decision-making,' its policy responses often lag behind the available evidence in many fields. The relative lack of investment in home care for seniors is a prime example.)

It is essential to interject here that the current study is the first of the series of studies which incorporates ideas with policy making. This will be followed by newer interpolation of ideas that need to be integrated with differing aspects of policies to be formulated to securitize national security policy making, enhance its robustness as a composite whole and pave the way to achieve "Jointness" essential in conducting the military affairs in the 21st Century.

POLICY JUXTAPOSED AGAINST DOCTRINE, LAW, PROGRAM OBJECTIVES, GUIDELINES & THEORY

What is the difference between a policy and a doctrine?

"policy" and "doctrine" aren't opposites — they're not even on the same axis. Doctrines are beliefs that are taught (in fact, the word "doctrine" comes from the Latin for "teachings", suggesting that any belief taught in the church is, at some level, doctrine). Policies are organizational practices. Some doctrines are policies, some policies are doctrines, some are both, and some are neither. Determining that a particular teaching is policy doesn't necessarily mean that it's not also a doctrine.

Policy & Law

Laws are formal statements of government policy enacted by authorities accepted as legitimate by the societies in which they act. Policies are broader in the sense that they are either formal statements (rules) of acceptable practice or informal practices (norms) that constrain the activities of actors (persons, committees, board, etc.) within any organization, governmental or private.

Policies and Programs Differentiations

Policies are for the long term. However, if the goal is social equity, then programs are important. (Starsky Wilson 2015) Programs are short-term interventions that create temporary improvements in the wake of challenges. Policies, on the other hand, are covenants that the society chooses to live by, as articulated in legislation and regulation. In the ongoing struggle for social justice and equity, policies and programs can both be helpful tools. However, government officials and their constituents need to understand the distinctions between the two and the responsibility of governance for policy to institute real, progressive change. See the link.

http://www.governing.com/gov-institute/voices/col-social-equity-crucial-difference-policies-programs-ferguson.html

Differentiating policy from Objective and Guidelines

In a single sentence which becomes self-explanatory, a policy is what you do. The objective is why you do it. Further a policy is a specific set of rules and principles that is considered official constitutionally and is supposed to be implemented by everyone at a company, or by people in the government. Guidelines, on the other hand, are not official rules, and they may or may not become a policy one day. They are at the level of helpful suggestions, or good advice, or useful ways to get something accomplished. For example, there still does not exist any official "Defence Policy of India" but there are as Prime Minister Narasimha Rao stated in the Parliament that there are "Guideline" which are very diligently followed by the Service Chiefs and the Government and that these "Guidelines" are reviewed from time to time. We begin in this exposition the exploration of the "Defence Sector" because this sector presently has had a longer tradition of extrapolation. This will be followed by exploring other sectors in the succeeding monographs.

THEORY AND POLICY

Theory is the explanation of the observed behaviour-it is an answer to WHY. Theories are thus intellectual constructs of the objective realities formulated by the academicians according to their knowledge and foresight. While in case of sciences, theories are usually correct. However, in the case of the social Sciences they are subject to certain assumptions.

Therefore, on the basis of information available and making certain assumptions they explain the current situation, predict the future and make certain recommendations to the opinion makers and policy formulators. Since the assumptions are most of the time subjective in nature the, explaining the current situation, recommendations to be adopted or predicting the future is in accurate and fragile in character.

Policy is intention of the policy makers HOW to change those very conditions in accordance with their desires. It is set of rules and directions made by the practioners to change the future Thus the Keynesian theory of economics maintained that the global economic depression of the 1930s was due to less demand of goods and services as compared to the supply of these goods and services because people had no money to spend due to unemployment.

Accepting this as the true explanation of the situation, American government initiated massive programmes of infrastructure to create employment and thus give money to the people for spending on the goods and services. This is an example as to how a theory led to the formulation of a policy in the United states during the days of great depression.

WHAT FIRST Strategy Policy or Planning?

Which comes first - strategy, policy or planning? A. M Sufian wanted to dedtermine the difference between policy, planning and strategy. There has been a long debate about the same without any consensus that what comes first? Rationally, first you adopt a strategy to reach the goal and accordingly design policy and based on policy you make detail plans to achieve objectives. Could it be other way round by which you enunciate a policy and then adopt a strategy to achieve a goal or objective.

It is a difficult question to answer but rationally the order should be: policy, strategy and then planning. First you formulate a policy which is the principles or the protocols to guide decisions and next we can make a strategy and finally a detailed plan to achieve the strategy. Still it is a difficult question as they are all closely inter-related, and are all products of the process of planning. Strategy on the other hand a product of the process of planning, and it is defined as a long-term plan. Regarding the policy, if we define it as “deliberate course of action based on a definite plan or program created through a process of thought and reason” with goals, means, implements and constraints as it’s’ elements (Halcrow, 1984), then it would follow the strategy and the goals defined in it. The short and mid-term plans and programs are used for more detailed planning of the goals and objectives defined in the strategy. So they could come as more operational means for implementing the strategy (and policy adopted.

Therefore, one rationalization could be that data must come first, then create a strategy for delivering a policy and plans to be implemented. The flow chart would then be “Good data---> good strategy -----> good policy”

POLICY MAKING FLOW CHART

A self-explanatory flow chart on policy making is placed below

POLICY MAKING PROCESS

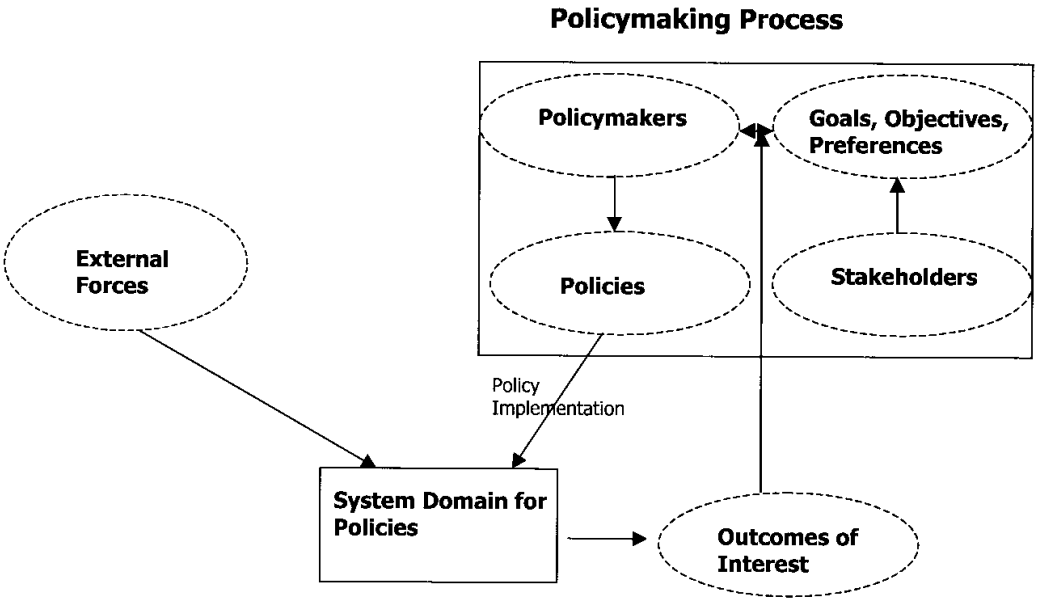


Figure 1. Elements in the policy analysis approach.

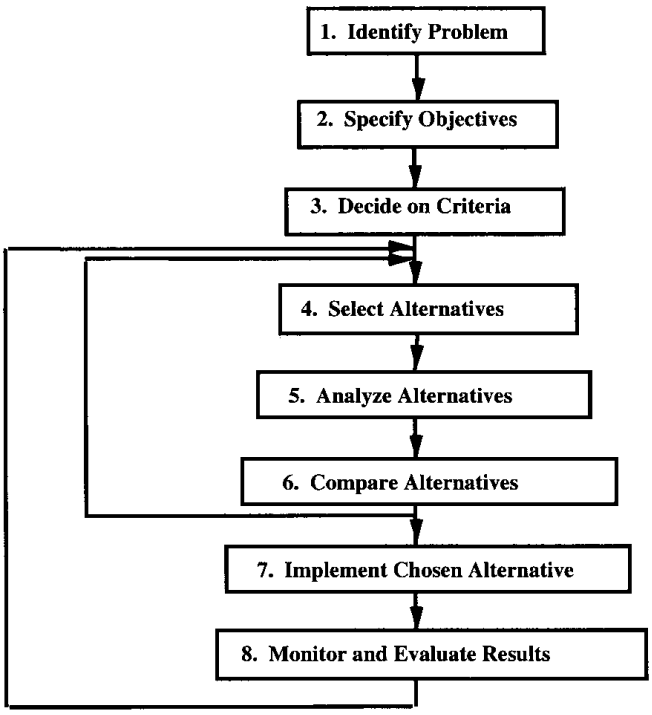


Figure 2. Steps in a policy analysis study

ANALYSIS OF KEY POLICY DOCUMENTS ON INDIA'S NATIONAL SECURITY AFFAIRS

For the purposes of this paper the following policy documents have been considered for critical analysis from a policy formulation perspective.

1. Swaraj in Ideas
2. Creation of Defence Planning Committee (DPC)
3. Cyber Security Policy 2013
4. Draft Defence Production Policy 2018
5. Joint Doctrine, Indian Armed Forces, April 2017

WHAT NEEDS TO BE INCORPORATED UNDER THE REALM OF IDEAS

All the four Policy Documents under review should have had a procedure to undertake out of box thinking to be integrated while composing the documents. All four documents have a direct relations to India's national interest and national security. Hence out of box thinking has to be done by experts from different fields of social sciences, management sciences and from the fields of natural sciences. These outside experts should not belong to any government organizations or even government funded think tanks to maintain the autonomy of thinking and maintaining the purity of the discipline to which they belong or have been trained.

1. Defining the concept of national interest and national security in epistemological terms to cover the broad contours of Indian civilizational and cultural values. India's national interest has now to function at two levels. First, at the internal federal level to safeguard the centre-state relationship and intra state relationship to eradicate any aspect which may cause conflict of interest at social, political, economic and strategic developmental levels. Here the role of a temporal historian with specialization in modern Indian history becomes essential.
2. Defining the epistemology of the concept of securitization becomes the key element to incorporate the policy document on cyber security. Hence the role of the experts from the field of political theory and political philosophy becomes essential.
3. Defining the philosophy of indigenization leading to the incorporation of self-sufficiency in defence production and hence fortify our national security becomes the key element to incorporate the realm of ideas for the policy paper on Defence Production. Hence the experts in the area of finance, management sciences, and commerce will be needed to give impetus to incorporate the role of the "realm of ideas".
4. Defining the purpose of power, use of force and creating a credible deterrence capability against all the adversaries of the Indian nation state would have been the terms of reference to create the policy paper entitled " Joint Doctrine, Indian Armed Forces, April 2017 (JDIAF). Hence the experts in the areas human resource development, management experts, financial experts, industrial production experts and scientists who have the understanding of converting "science of today into technology to be used tomorrow" should be contributing towards the realm of ideas for the JDIAF.

COMMENTARY ON DPC

There has been no release of any official document by the government on DPC. In the absence of any policy paper, the only information about its structure, the architecture of its organisation and duties that DPC is to perform is only known to the people of India is through the media report in various newspapers. Like the NITI AAYOG, the DPC has also been established through an administrative order and hence has no constitutional standing as the Chairman of DPC is the NSA and NSA as such till date is an appointment by an administrative order. Hence the creation of the DPC without any stakeholder from outside the Government and severely lacks any ability to incorporate any adventure in ideas nor it can its member have the luxury to postulate their notions to cover the realm of ideas.

Every major power of the world and more so the two superpowers in the post 1945 period had never ceased to carry out the intellectual and introspective methodology to bridge the gap between the realm of ideas and the domain of public policy making on matters of national interest and national security. This entailed that the best of brains from the government organizations to those belonging to corporate sector and the academia participated.

No nation state's history is so un-chequered and as ambiguous on matters of national security as that of India. However, VP Singh Government in 1991, created the National Security Council and the National Security Advisory Board (NSAB). It never got operationalized though its membership included the members of the government and the public intellectuals from the academia and think tanks. Further on record is the statement of P V Narsimha Rao in 1996, the then PM and Defence Minister, on the floor of the Parliament, that there was no official document called "India's Defence Policy" but only guide lines. It was the Bajpai government in 1999 which constituted once again the National Security Council(NSC) the National Security Advisory Board (NSAB), established the National Security Council Secretariat(NSCS) and made them functional too by instituting the post of National Security Advisor (NSA). Since then, NSCS, the NSAB and the four successive NSA have taken charge of their offices. However, the entire edifice has been created by an administrative order like it was in the case of the Planning Commission of India and not by an act of the Parliament. Its role has been advisory and its future hangs on balance in terms of its permanency depending on the political outlook of the Head of Government. While the NSAs have enjoyed personal confidence of the Head of Government, yet they remain unaccountable to the Parliament as none have been the elected members of the House. Hence the entire architecture suffers from unaccountability as well as having an "Achilles Heel" far larger than the smaller area that was part of Achilles's foot. The size of the NSAB historically fluctuated representing a healthy mix of expertise which had the potential to bridge the gap between the realm of ideas and the domain of public policy making. This potential was hardly utilized and its size dwindled to nearly a skeleton size in post 2014 period with the position of the Chairman NSAB further diluted and renamed as Coordinator. The result has been that the entire workload of National Security related matters have rested on the NSA with the assistance of the Deputy NSA and his staff of NSCS.

Enter DPC

For 70 years the governments in power have been tacticising strategy and the NSAB has been an unemployable organizational headache. Hence it had become essential to revitalize the NSCS to its full potentials.

For India to meet the challenges of Security in the 21st Century, the Government announcement of 18 April to establish a Defence Planning Committee (DPC) under the Chairmanship of National Security Advisor Ajit Doval can be considered to be a game changer. Hindustan Times reported that

> "The Chief of Integrated Defence Staff to the Chairman of the Chief of the Staff Committee (CISC) will be the member secretary of the committee, according to the notification, and the HQ of the Integrated Defence Staff will be the secretariat of the DPC."

DPC will consist of the Chairman Chiefs of the Staff Committee (COSC), service chiefs, Defence Secretary, Foreign Secretary and Secretary (expenditure) in the Finance Ministry. The Committee will operate through four sub-committees to cater for (1) Policy and Strategy (2) Planning and Capability Development (3) Defence Diplomacy and (4) Defence manufacturing ecosystem. The Indian Express reported that

> "the DPC has been tasked to undertake external security risk assessment and define national defence and security priorities. It will also formulate the national military strategy, a strategic defence review and a draft national security strategy. To accomplish these requirements, DPC will identify the "means" and "ways" across ministries, obtain CCS approval for a capability development plan and provide guidance for budgetary support. The DPC will also prepare a roadmap to build a defence manufacturing ecosystem, a strategy to boost defence exports and prioritized capability plans for the armed forces in consonance with the overall priorities, strategies and likely resource flows. It will submit all its reports to the defence minister."

While it is too early to comment or foresee the events that will unfold with the DPC in place, yet the contours of important fall out can be visualized. The Government is determined to

1. Allow the architecture to function as a base for providing inputs in the policy making on national interest and national security strategy.
2. DPC will not be allowed to become routinized or bureaucratized.
3. The ambiguous nature of defence policy will be eradicated. The intent and objectives of India's national security strategy and policy making will be backed by the political will of the Government.
4. Consensus between the Service Chiefs and the Chairman of the Chiefs of Staff Committee will be enhanced as they will all sit as a part of DPC. This will also enhance the philosophy of "JOINTNESS"
5. The Government is well aware of the fact that the members of the DPC and Sub-Committees are all part of the establishment and hence in essence the Government is only hearing from itself. There is bound to be some mid-course correction given to enhance the process by which talent and expertise from outside the government agencies will be brought in in a calibrated way to fortify the realm of ideas to enrich

the domain of public policy making.

6. Lastly, there is hint when one reads between the lines that the creation of the post of the Chief of the Defence Staff may be of serious consideration by the Government.

One can at this moment of time wish the Chairman of the DPC in general and the NSA as an individual all the best to implement the game changer. Observing the way, the present head of government has been operationalizing the functioning of national security strategy architecture, the nodal point which will contribute to decision making will be the role of the NSA and his professional competence to smoothen out the rough edges of such a group assembled under one roof. Hence the NSA has to be empowered to work to strategize at global level to ensure that domain expertise of members of DPC does not precipitate "tacticising of strategy". The formation of the DPC at that time had effectively stalled the creation of the CDS and Ajit Doval the NSA had been de-jure and defacto the unofficial CDS.

COMMENTARY ON CYBER POLICY

The entire Government of India document on Cyber Security at Appendix is based on the premise that ICT will be used to secure Cyber Space and hence achieve the vision and aim of cyber security in the country. The policy paper does not even touch upon the necessity to securitize the domain of cyber space nor does it dwell upon the theoretical construct of securitization as developed by the Copenhagen School in the early 1980s. Copenhagen school was the first to record through its research and deliberations the method to bridge the gap between the realm of ideas for universal securitization and the domain of public policy making for the emerging cyber space and cyber security. Unlike in the 20th century when security was narrowly focussed to preserve the "state" by the use of technology, the domain of cyber space and cyber security has a much more complex interplay between the cultural and international political economy at the national and transnational levels. Appended below is the fundamental deliberation on the normative aspects of cyber security which must be the main stay of the Government of India policy on cyber security.

The Normative Aspects of Cyber Security

"***Theory can never supersede experience and judgement but theory catalyzes both***."

For two years in succession at the FICI, the plenary speakers have had the privilege to address the august gathering of experts and thinkers from across the spectrum of policy makers, industrial leaders, management experts, technocrats and public intellectuals. One year's theme on internal security made it possible to focus on an Indo-centric approach and tailor make the deliberations related to India's specific needs and thus locate the normative aspects to further them for Indian utility. However, the second year's deliberations "make in India for cyber security" does not only imply "made for India" but also has the potentials to create an organic global linkage with every nation of the world. Hence the scope is vast, transnational in nature, multi-disciplinary in format to create an integrative methodological model based on empirical methods to account policies made in an accountable way. Policy is always the outcome of opportunities and resources in which the opportunities have to be credible and resources have to be adequate. If one evaluates the phenomenal advances made by China as the manufacturing hub of the world, it is because they deeply introspect what

policy ought to be to achieve their national interests at two levels. First, at internal national level and second at global competitive level.

Today China's Cyber Security operates through Cyber Forces at three levels, consisting of Military Network Warfare Forces, Authorized Teams of Network Warfare Specialists and Non-Governmental Forces. Their conceptualization of Cyber Security operating in a global cyber space makes them the leaders in the world. Their Cyber policy takes into account not only the cultural preconditions of their own country but of the rest of the world. Their Cyber policy is culture as well as ideology driven, rather than only technology driven. They are not reacting to the world at large but they are making the world react to their policies, global interests and their notion of the future balance of power. They are using technology as a tool, the security forces as a means and their ambitions to become a recognized world power second to none as the driving force. They thus see cyber space and securitization of cyber security as essential to preserve their cultural and ideological moorings which is highly subjective in nature.

In essence at a universal global level comprehending cyber space is imminent and enveloping as space itself. It has no respect of any boundaries whatsoever. That being the case the protection and promotion of national security interest in cyber space calls for vision and technological advances. Vision is another name for bold imagination and every problem that is foreseen will be solved provided there is a follow-up action and dedicated application. The worst that a nation can do in these circumstances is to follow an ostrich in sand policies. There is no time to loose.

GLOBAL OVERVIEW

At the Davos Economic Meet in 2016, an interesting panel discussion was held to discuss as to how the world will have to live in the twenty first century. There were six participants. Only one amongst all the other economic experts was a lone international relations expert Sir John Chipman heading IISS a British think tank. Each spoke for five minutes before it was open for discussion and QA session. Chipman stated that "the world in the 20th Century lived tactically but in the 21st Century the world will have to live strategically". What it meant was that the concept of security through tactical means have to give way a larger concept of the epistemology of "securitization" which was developed by the Copenhagen School in the early 1980s. Copenhagen school was the first to record through its research and deliberations the method to bridge the gap between the realm of ideas for universal securitization and the domain of public policy making for the emerging cyber space and cyber security. Unlike in the 20th century when security was narrowly focused to preserve the "state" by the use of technology, the domain of cyber space and cyber security has a much more complex interplay between the cultural and international political economy at the national and transnational levels.

If during the coming few years of deliberations, we can have a consensus on what is the definition of cyberspace and what it will take to "securitize" the cyber space then we have taken the first baby step to understand the issue of securitization and as to why it has universal application at regional and global levels. The process of securitization is intrinsically linked to the avoidance of war and maintaining of peace. Occurrence of War and achieving Peace are cultural phenomenon and hence have no technical solutions. While War and Peace could be localized in its occurrence depending on the situation, the circumstances

as well as the leadership under which it functioned or occurred, Cyber space cannot be similarly confined or managed. The beginning of the cyber space is global, in nature universal and applicable to the smallest of nation states to the entire comity of nations which are interconnected today because societies have become digitized.

Important to note is that what was first invented by Pentagon's Advanced Research Projects Agency in the 1960's for military purposes and later developed by a British software engineer has changed the way we communicate, work and interact and has "come to characterize modern life" (Barett et al., 2011: 34). The World Wide Web was introduced in 1991 and now a majority of societies have become digitalized and are connected to what we call cyberspace. Much has happened since 1991 and cyberspace has come to dominate all parts of modern society. There is still no universally accepted definition of cyberspace, as it encompasses everything from software, hardware, the Internet, information, cables, servers, computers, interaction between individuals, states, companies and cultures. Therefore, cyberspace is somewhat a floating concept that is difficult to grasp. However: "the narrow meaning of the term (cyberspace) is the electromagnetic spectrum by which digital data are transmitted".

Digital communities have also become a new factor within world politics and therefore also a new power element within the balance of sovereignty. Moreover, the use of the Internet expanded at an annual average rate of 290 per cent globally from 2003 to 2009 and has become the core component of everyday conduct for all actors within our society. It is estimated that in 2020 sixty per cent of the world's population will have access to the Internet. Fifty billion physical objects and devises will be connected to the Internet, which amounts to ten devises per online individual. Loss of access to the Internet will have critical consequences to the prosperity of a nation. Cyber-attacks are politically and economically motivated and are also being used for purposes of industrial and state sponsored espionage in an increasing rate.

President Obama stated in a speech of May 29th 2009 that "cyber threat is one of the most serious economic and national security challenges we face as a nation (…) economic prosperity in the 21st century will depend on cybersecurity". In 2012, there were reported 47,000 security incidents, 621 confirmed data disclosures, and at least 44 million compromised records in the US, which is a trend that spans across the world. Since 2012, internet users have been growing between 20% to 30 % every year and today here are some 2.5 billion users world-wide and digitalization has become such an integrated component within our society that it has become a global common caused by the borderless nature and global accessibility of cyberspace. Internet is thus used by all and owned by none.

The word 'cybersecurity' is widely used as a term for protection against malware and hacker attacks. It is often used situationally, in the sense that an individual's connected devices can be under attack, a corporation can be hacked or government-run, essential infrastructure can be at risk of attack. But it seems that the broadness of the term may have made an exploration of the theoretical aspects of cybersecurity difficult. Not many attempts have been made to understand cybersecurity from a higher level of abstraction. In this paper, it is stated that the broadness of the term is indeed appropriate, as cybersecurity is a multi-faceted phenomenon which nonetheless can be analyzed theoretically across all levels. The meaning of the term is explored further and an attempt to widen and deepen its reach as a concept is made. Cybersecurity is explored from a critical security studies angle as well as a critical theory angle. A distinction of the term from related concepts such as information

security and computer security is put forward, and a taxonomy of cybersecurity is suggested. It is concluded that cybersecurity must necessarily be analyzed critically in order to fully understand the impacts and implications it has as a phenomenon, but that this analysis will inevitably lead to a multi-faceted, yet meaningful result.

Cybersecurity is a shared responsibility. Every Federal government has the responsibility to protect and defend the country and we do this by taking a whole-of-government approach to countering cyber threats. This means leveraging homeland security, intelligence, law enforcement, and military authorities and capabilities, which respectively provide for domestic preparedness, criminal deterrence and investigation, and our national defense. Yet much of our nation's critical infrastructure and a diverse array of other potential targets are not owned by the Federal government. The Federal government cannot, nor would it want to, provide cybersecurity for every private network. (The White House, 2015)}

The Context

The concept of securitization is generally associated with the Copenhagen school of security studies, which is generally taken to include Ole Wæver, Barry Buzan, and a range of other, more loosely associated, researchers. Originally devised by Ole Wæver, the concept of securitization provided a fresh take on the increasingly tiresome debate between those who claimed that threats are objective (i.e., what really constitutes a threat to international security) on the one hand, and those that maintained that security is subjective (what is perceived to be a threat) on the other. In an attempt to sidestep or bypass this debate, the Copenhagen school suggests that security should instead be seen as a speech act, where the central issue is not if threats are real or not, but the ways in which a certain issue (troop movements, migration, or environmental degradation) can be socially constructed as a threat. The idea of speech acts has a long tradition in philosophy and refers to the idea that by saying something, something is done. So, just as the naming of a ship is a speech act that brings something into effect, the uttering of "security" can be viewed as an act by which all kind of issues (military, political, economic, and environmental) can become staged as a threat. However, not all talk about security qualifies as securitization in the sense understood by Ole Wæver and his Copenhagen colleagues.

A securitizing speech act needs to follow a specific rhetorical structure, derived from war and its historical connotations of survival, urgency, threat, and defense. This leads the Copenhagen school to define securitization as a speech act that has to fulfil three rhetorical criteria. It is a discursive process by means of which an actor (1) claims that a referent object is existentially threatened, (2) demands the right to take extraordinary countermeasures to deal with that the threat, and (3) convinces an audience that rule-breaking behavior to counter the threat is justified.

In short, by labelling something as "security," an issue is dramatized as an issue of supreme priority. One can therefore think of securitization as the process through which non politicized (issues are not talked about) or politicized (issues are publicly debated) issues are elevated to security issues that need to be dealt with urgency, and that legitimate the bypassing of public debate and democratic procedures. The Copenhagen school originally studies the dynamics of security across five different, nonexclusive sectors:

1. Military
2. Political

3. Societal
4. Economic,
5. Environmental

However, later analyses of securitization have sought to expand the number of sectors. Because securitization enables emergency measures outside democratic control, the Copenhagen school generally opts for De-securitization, rather than securitization, as the preferable mode of problem solving.

Research Methodology and Philosophy for Cyber Security

Methodology

A methodological approach to the research field of cyber security is important, as we want to explain where the topic originates from and why we are conducting our research in a particular way. We will therefore account for how the research has been conducted, for what methodological reasons, in addition to explaining what effects the choice of method has for the research findings.

Therefore, our efforts must account for the methodological reflections related to our research question and their theoretical basis. One has to start out by clarifying our philosophical stance to the research topic, our research approach and our research design and strategy. Hereafter, the methods for the data collection and its effects on the reliability and validity of our findings will have to be discussed. Lastly the delimitation of our research must be addressed.

National Security

National security refers to the safety of the territory and population of a nation-state and by extension, to the policies adopted by its preservation (Paleri, 2008). For some academics national security is a "constructed concept" for any nation-state at any given time. Multiple factors, like political priorities and the media, will play a role determining what issues must be securitized; those issues and are known as "security priorities" (Richards, 2012). Seen as the "national interest," security priorities may change according to the nation-state's geopolitical position or external conflicts (Bobbitt, 2002; Richards, 2012).

Theoretical Framework

The theoretical framework used here is the "Securitization Theory of the Copenhagen School," also known as "securitization theory". This theory argues that security is a constructed concept, a specific type of politics applicable to a very broad set of issues in certain time (Buzan, 1998). The securitization theory defines security as a "speech act that securitizes," and constitutes one or more "referent objects," which can be identified as the national interest. This theory has been selected for this paper because the political speech about securitization has been oriented to construct "cyber issues" as "security problems," rather than regular political, economic, illegal or technical problems (Hansen, 2009; Williams, 2003). Using the terms of the securitization theory, this paper has the purpose of exploring the different justifications governments used in shutting down the Internet, an "extreme measure" to protect what they consider the "referent object," in order to guarantee the national security of a nation state. The securitization theoretical framework identifies the

following elements:

1. Securitizing Actor: whoever "securitizes" something,
2. Referent Object: thing to be protected,
3. Audience: person to be convinced with the security speech
4. Extraordinary Measure: action (s) to protect the referent object.

Research philosophy

The term research philosophy is related to the "development of knowledge and the nature of that knowledge" (Saunders et al., 2007: 101). The research philosophy chosen and adopted includes:

1. Important assumptions of how we see the world, and
2. How these assumptions will therefore support our choice of research strategy
3. Methods of obtaining knowledge.
4. Important epistemological considerations to reflect upon what we consider to be acceptable knowledge in the field of study as enumerated below.

According to Abbott (2004) there are two main strands of social sciences; positivism and interpretivism.

Positivists believe that meanings in social life can be measured and that research is replicable and comparable, and is therefore independent of context (Abbott, 2004). In this case they take the philosophical stance of natural scientists, as they will be "working with an observable social reality and that the end product of such research can be law-like generalizations similar to those produced by the physical and natural scientists" (Remenyi et al., 1998, in Saunders et al., 2007: 103) and can most generally be seen within the natural sciences.

Interpretivists, on the other hand, rely on meaning through interaction and interpretation; thereby the emphasis in interpretivism is on the meaning of social life and not the measurement. Interpretivists argue that it is not possible to measure social life and that it is therefore not possible to decontextualize or universalize research results (Abbott, 2004). They argue that it is essential for the researcher to acknowledge that the world is socially constructed and understand the difference between humans in our role as social actors. According to interpretivists the world and the meaning of something is subjective, and an objective view of the world is therefore impossible. Different phenomena are not only complex, they are also unique and it is therefore necessary to look at the totality in order to understand social phenomena.

As we are looking at securitization of cyber threats, hence what security means, which indeed is contextual, have to take an interpretivistic approach to the research conducted. Securitization is a study of discourse, and thus based on language, which is clearly linked to interpretation. Looking at the issue through an interpretivistic approach is therefore needed. The interpretivistic approach will thereby help us in understanding how cyber security is regarded and what should be done in order to deal with the issue. Our epistemological stance of this research presentation will have to follow the interpretivist view where our ontological position is the one of constructivism, as we are analyzing cyber security with an ethnographic approach. An ethnographic approach is highly interpretivistive according to Abbott, and we

have chosen to use the approach because of the highly sensitive information that cyber security deals with (Ibid.). Cyber security is also an area that has a very secretive culture and the people involved are very hesitant to talk and discuss the issue. Therefore, an ethnographic approach will enable us to meet and create personal connections, which will benefit how we collect the information we need to analyse the choice of subject.

Constructivism believes that "social phenomena are continually reproduced in interaction" (Ibid.:52), which is the core of speech act theory, a part of our theoretical basis of this research. Furthermore, according to Steinar Kvale and Svend Brinkmann (2009) a phenomenological approach has a clear prevalence in qualitative research, such as the one we are conducting. This is a term that points to an interest in understanding social phenomena from the actors´ own perspectives and describing the world as experienced by the subjects, with the assumption that the important reality is what people perceive it to be (Kvale & Brinkmann, 2009: 26), relating to our interpretivist approach. Social science tries to explain social life (Abbott, 2004). The aim is to unfold cyber security and explore the issues of the securitizing process and explain this through empirical data.

The world of cyber security is fast changing and we therefore encourage further study in this interesting field, because cyber security has a very unique, important and challenging part of our society that we believe will increase in importance. Like Abbott argues, "Knowledge is always situated" (Ibid.: 50), and therefore we are aware of other forms of potential outcome, but the study will give a picture of similar situations.

Strategizing Public Private Partnership Model

A successful cyber security policy will entail a Public Private Partnership model in which the product (Cyber Security Policy) will have to be enunciated threadbare by the government in power so that the academia can introspect in the realm of ideas and the industry can formulate the methods by which the dots and dashes between the "product" and "ideas" can be integrated by the industry to operationalize a full proof and fail safe cyber security policy. The national security perspectives of a nation state can then decide how to implement the same at the level of its own national interest at internal and global external levels. Thus synergization of the government elements with that of the notion in the realm of ideas generated in the academia and the operationalization of methods by the industry to create the final product called the "cyber security policy" based in a PPP model.

As the academia by the very nature of its operational existence has no mechanism for revenue generation, the fiscal and financial aspects has to be borne between the government and the industry in a forty sixty ratio with a clear understanding and acceptance that failure of product delivery at the industry level at functional levels (by the industry) or shortfalls in the realm of ideas at cognitive levels (by the academia) will be acceptable by the government and the industry and will not become an impediment for the continuation of the PPP model for perspective planning to devise the cyber security policies that will have to operate in the changing atmospherics of legal, political, social and economic circumstances within the international environments continuously in the 21st Century.

CYBER SECURITY CHALLENGES

What is cyber /computer/information Security?

1. Security under cyber space
2. The branch of Security dealing with digital or information technology.
3. Is the prevention of unauthorized access and/or damage to computer systems via internet access.
4. Entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption.
5. Involves protecting that information by preventing, detecting, and responding to attacks
6. How much of your personal information is stored either on your own computer or on someone else's system?
7. Building confidence on the use of ICT

Cyber Security & Legal Issues

1. Cyber Security is another key area that raises legal issues such as cyber crimes
2. Cybersecurity is one of the most profound challenges of our time.(Theft of identity, hacking, cyber-terrorism, e-financial crimes)
3. The costs associated with cyberattacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial of-service attacks and network outages.
4. Some use ICT benefits to the detriment and harm of others.
5. Technology facilitates the commission of "old fashioned crimes" such as fraud, theft, money laundering, terrorism etc.
6. Technology creates new illegal activities such as computer hacking, distribution of computer viruses, unsolicited emails and other related computer misuse
7. Easy to manipulate information online. Internet removes the geographical boundaries

Challenges on Cyber Security

1. Lack of Legal Framework at national and Regional Level (EAC& Africa)
2. Nature of offences
3. Nature of cyber space
4. Lack of Knowledge on computer forensic & e-evidence
5. Admissibility of e-evidence Jurisdiction problem on enforcement

Examples of Cyber or computer crimes

1. Fraud, hacking, theft of data/information, e-financial crimes, phishing,
2. Cyber-terrorism, cyber-corruption cyber-stalking, e-child grooming, e-child pornography, spoofing attacks, defacement attacks
3. data theft, payment fraud and other related frauds, software and data theft unsolicited emails, distribution of e-viruses, publications of obscene materials
4. Do our Laws carter for these e-offences?
5. The UK Computer Misuse Act 1990 deals with cybercrimes, jurisdictions and extradition

Facts and Figures for Cyber Crimes:

Cybercrime is worth an estimated 105 billion dollars and cybercriminals can earn around USD 23,000 a week.(rival computer security firm McAfee)
Several computer security consulting firms estimate global financial losses from viruses, worm attacks and other hostile computer-based attacks to be between $13 and $226 billion. (the Congressional Research Service)

Governance, Management, and Normative Models of Cyber Security

Cyber security refers to all the approaches intended to protect data, systems and networks from deliberate and accidental attacks and yet, if required, from the lack of preparation for the recovery of these infrastructures (MIT, 2011). It is a collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices and technologies that can be used to protect the cyber environment as well as the assets of the users and organizations (ITU-T,2008). Unlike the conventional models of information security, the objective of cyber security is to reduce the risks concerning the dependency of the cyberspace and the presence of adversarial threats (Bodeau et al., 2010).

Two constructs of cyber security are pivotal to this study: governance and management. The term governance is used to describe a system for controlling or regulating, which includes the process of naming controllers and regulators. Whereas the term Management is adopted to refer to the communication of the responsibilities of controllers and regulators, by using executive actions (Turnbull, 1997). Governance consists of the definition of criteria for decision-making, setting rules, responsibilities, and the boundaries of the autonomy and actions of the involved parties (Roth et al., 2012). The role of governance is not managing, but defining the scope of management. Considering cyber security, the governance focuses on what the organizations should do differently or adding to what is accepted as good information security governance practices. Using this methodology, the level of readiness of the organization for cyber security is analyzed under the perspective of the following approaches (Bodeau et al., 2010): strategic integration, extending the cyber security strategy beyond the organizational environment, risk mitigation, adaptability and agility in decision making to face cyber-attacks against corporations, senior engagement and commitment from the shareholders and the board of directors and cyber risk analytics.

As of the strategic integration dimension, it is discussed to what extent the cyber security strategy is integrated with other strategies, the mission and risk management of the organization. The perspective of adopting strategies that use resources originating from external environments refers back to the commitment of the company with its partners, suppliers and customers to share knowledge about threats that may affect the organizational activities. In the approach towards mitigating the cybernetic risks, the reference is structuring actions to prevent threats in a normative view of the best practices to avoid unpredicted attacks. Regarding the variable agility in decision making, the conditions provided by the organization to delegate responsibilities in fighting the interests of competitors in violating the cyberspace of the organization are observed. The dimension commitment of the board of directors indicates the involvement of shareholders, counsellors and executives in monitoring the implementation of cyber security actions. Finally, in the analysis of cybernetic risks, it is discussed how the models of threats to the organization environment should be managed and updated (Allen, 2005; Bodeau et al., 2010). In this scenario of cyber security governance, it is

still possible to list the recommendations for corporate governance of the OECD - Organization for Economic Cooperation and Development (OCDE, 2004). The document shows the importance of respecting the interests and providing equitable treatment for shareholders; transparency, quality and integrity when releasing information; making use of the responsibilities of the executive board; improving the compliance with legislation; and the effectiveness of regulatory and supervision agencies in monitoring the activities of the sector. By means of recommendations and guidelines from the OECD it is possible to elaborate on a set of dimensions from corporate governance applied to cyber security governance for smart grids, as follows:

1. The effective legal and regulatory basis in cyber security governance for Smart Grids;
2. The relations with stakeholders of Smart Grids in cyber security governance
3. The rising standards of transparency in accordance with corporate governance principles of cyber security management for Smart Grids
4. The equitable treatment of shareholders
5. The responsibilities of the Executive Board in energy utilities regarding cyber security governance for Smart Grids.

In the outline of governance, cyber security management has ANSI/ISA99 (America National Standard Institute) as a normative pillar since it handles security in industrial automation and over the years it has become a key international standard to enable the protection of critical industrial infrastructures. It is a normative management instrument that directly influences the security and health of people and the environment. Probably in the near future, they will reach other areas of application, wider than the ones towards industrial automation. For operating cyber security management, actions beyond projects are required from the organizations in order to enable the achievement of a higher security level for their processes. The continuous management of security issues is a demand to keep the desired level. Projects are capable of raising the security level however keeping it is improbable using initiatives that are not often aligned with the strategy of the organization. The effective implementation of a cyber security program comprises effective risk management, system development and its maintenance, management information, planning and being able to respond to critical incidents (ANSI, 2009). It is also worth adding the need of preparing and qualifying the human resources involved.

Based on the cyber security governance and management dimensions and identified through the models mentioned as theoretical references, a theoretical-methodological model can be elaborated and can be adopted for the investigative process and field research.

RECOMMENDATIONS

1. We need to convert the enquiry of cyber security into a discipline based on theory with a paradigmic status.
2. We must create a consensus about the definition of cyber security.
3. Our enquiry in cyber security should not be reactive but proactive.
4. Identify risks from cyber security in the basis of a clear understanding of our cultural and civilizational perspectives.
5. Synergize the efforts of the practitioners, the corporate sector and the academia by creating a Public Private Partnership Model.
6. Bridge the gap between the realm of ideas and the domain of public policy making

COMMENTERY ON

Draft Defence Production Policy 2018 (DDPP)
And
Joint Doctrine, Indian Armed Forces, April 2017 (JDIAF)

Draft Defence Production Policy 2018 (DDPP)

The DDPP was released as a draft in early 2018, and Comments were requested to be provided at dirpnc-ddp@nic.in latest by 30.03.2018. The Draft has been placed as Appendix-D. It must be noted the DDPP has been issued at regular intervals since 2003.

There has been no policy document that has been issued till date. It also does not indicate as to who were the Committee Members under whom the document was prepared. Hence the possibility to articulate as to whether the "realm of ideas" could be considered to be incorporated is not possible. However, the following observations can be made:

1. It is a policy paper in the making
2. It can be conjectured that no outside experts belonging to the private, corporate or academia has been considered to be stakeholders.
3. The list of 22 issues is almost a unachievable wish list.
4. Serious questions related to as to why Defence Production failed to take off in the post independent period even till date has not been raised.
5. The paper does not indicate any method or methodology to be incorporated by which the Private Sector can become the real producer of Defence Equipment.
6. The paper does to strategize as to how the R&D for Defence Production can be shifted to the Private Sector.
7. Considering that the Defence Forces continue to require cutting edge technology to be incorporated to be able to meet threat to the nation state, there is no attempt to indicate as to how future requirements are to be met through indigenous production means.
8. The paper does not indicate whether any steps will be taken by which the user is incorporated in the system to monitor any form of defence production undertaken.
9. There is no indication that the Government will be able to accept the challenges and more so the failures associated with in the entire spectrum
10. Considering the way the DDPP has been set up there is hardly any scope for radical changes in the procurement policy

Considering the above factors and observations very little change can be perceived to be incorporated in future where the bridging the gap between the Public and the Private sector can take place. The question of stake holders who will represent the incorporation of realm of ideas for public policy is indeed far away.

Joint Doctrine, Indian Armed Forces, April 2017 (JDIAF)

Perhaps the most unusual document ever produced is the JDIAF 2017. In the very second page after the cover page it notes within the confines of the copyright symbol that "No parts of this book may be reproduced in any form by print, photo print, microfilm or other means without written permission of the publisher. Published by the Directorate of Doctrine. Headquarters Integrated Defence Staff". In other words the document cannot be quoted or cited as reference without first getting the written permission of the publishers. Considering the fact that the Chairman COSC had himself released the document in front of the press, the entire purpose of the document to be a referral document becomes self-contradictory. In page 4 it records that "This doctrine is pitched at military strategic levels, is meant to guide all members of the Indian Armed Forces ……. Is to be part of the initial training curriculum and should be revisited at all subsequent stages of training". The document hence does not leave any scope for intellectual critical review by any scholar, organization or even in a conference for any form of spontaneous debate or exchange of ideas. Also the document does not fulfil the stated purpose.

The Document gives a clear impression that it has addressed in general to even people in and out of uniform at the same time but with the directive that it can neither be quoted or referred or even cited. It is with this view that we have refrained from quoting or citing from the main body of the document and only taken the liberty to quote the matter from outside the main body of the document. However, reading the document gives the reader a feeling that the contents does not fulfil the stated purpose.

As the document is available in the net, the link is being placed as ANNEXTURE-E for any reader to be able to access the full document. It must also be noted that while the document does no harm whatsoever except causing serious confusion in the minds of young officers. Any further expression of the opinion on the document will not be appropriated as of now taking into considerations the directive in page 4 quoted above.

CONCLUSION

This research endeavour has been to synergise the content and context of theory with public policy making by examining four documents. The method has been an open ended exposition essay for the future generation of researchers from the academia, the professionals, the bureaucrats and the policy makers at all level to introspect as to how each one of them can attempt to interject the notion of bridging the gap between the realm of ideas and the domain of public policy making. No nation can achieve the stature of a major power unless the system, the organisations and the individuals help to synergize the ideas with policy making. It is strongly recommended that all future policy documents must at the time of their formulations must incorporate out of box thinking by a process in which fresh inputs are endorsed from the realm of ideas as enumerated earlier in the deliberation of this paper.

…..

APPENDIX – A

Swaraj in Ideas

Swaraj in Ideas – Krishna Chandra Bhattacharya Given below is the text of a lecture delivered by Krishna Chandra Bhattacharya (1875-1949) in October 1931 under Sir Ashutosh Memorial Lectures series, organized at Chandernagore by Charu Chandra Roy. (As the lecture contains some ideas and views of the great philosopher likely to stimulate thinking in our own day, it was considered worthwhile to resuscitate it from his old papers and present it before our readers.) From Visvabharati Quarterly 20, 103-114 (1954)

We speak today of Swaraj1 or self-determination in politics. Man's domination over man is felt in the most tangible form in the political sphere. There is however a subtler domination exercised in the sphere of ideas by one culture on another, a domination all the more serious in the consequence, because it is not ordinarily felt. Political subjection primarily means restraint on the outer life of a people and although it tends gradually to sink into the inner life of the soul, the fact that one is conscious of it operates against the tendency. So long as one is conscious of a restraint, it is possible to resist it or to bear it as a necessary evil and to keep free in spirit. Slavery begins when one ceases to feel the evil and it deepens when the evil is accepted as a good. Cultural subjection is ordinarily of an unconscious character and it implies slavery from the very start. When I speak of cultural subjection, I do not mean the assimilation of an alien culture. That assimilation need not be an evil; it may be positively necessary for healthy progress and in any case it does not mean a lapse of freedom. There is cultural subjection only when one's traditional cast of ideas and sentiments is superseded without comparison or competition by a new cast representing an alien culture which possesses one like a ghost. This subjection is slavery of the spirit: when a person can shake himself free from it, he feels as though the scales fell from his eyes. He experiences a rebirth and that is what I call Swaraj in Ideas.

In these days when our political destinies are in the melting pot, one is tempted to express a doubt – till now vaguely felt but suppressed as the uncultured – how far generally we have assimilated our 'Western' education and how far it has operated as an obsession. Certainly there has been some sort of assimilation – at least by some of us – but even of them it may be asked whether the alien culture has been accepted by them after a full and open-eyed struggle had been allowed to develop between it and their indigenous culture. It is admitted today – what was not sufficiently recognized in the earlier days of our Western education – that we had an indigenous culture of a high degree of development, the comparative value of which cannot be said to have been yet sufficiently appraised. Under the present system we generally receive Western culture in the first instance and then we sometimes try to peer into our ancient culture as a curiosity and with the attitude of foreign oriental scholars and yet we say that this ancient culture of ours is no curiosity. Many of our educated men do not know and do not care to know much of this indigenous culture of ours, and when they seek to know, they do not feel, as they ought to feel, that they are discovering their own self. There is no gainsaying the fact that this Western culture – which means an entire system of ideas and sentiments – has been simply imposed on us. I do not mean that it has been imposed on unwilling minds: we ourselves asked for this education, and we feel, and perhaps rightly, that it has been a blessing in certain ways. I mean only that it has not generally been assimilated by us in an open-eyed way with our old-world Indian mind. That Indian mind has simply lapsed in most cases for our educated men, and has subsided below the conscious level of culture. It operates still in the persisting routine of their family life and in some of their social

and religious practices which have no longer, however, any vital meaning for them. It neither welcomes nor resists the ideas received through the new education. It dares not exert itself in the cultural sphere. There can be no vital assimilation, in such a case, of the imposed culture. And yet the new ideas are assimilated in a fashion. They are understood and imaginatively realized; they are fixed in language and in certain imposed institutions. A drill in this language and in those institutions induces certain habits of soulless thinking which appear like real thinking.

Springing as these ideas do from a rich and strong life – the life of the West – they induce in us a shadow mind that functions like a real mind except in the matter of genuine creativeness. One would have expected after a century of contact with the vivifying ideas of the West that there should be a vigorous output of Indian contribution in a distinctive Indian style to the culture and thought of the modern world, -- contribution specially to the humane subjects like history, philosophy or literature, a contributions such as may be enjoyed by our countrymen who still happen to retain their vernacular mind and which might be recognized by others as reflecting the distinctive soul of India. Barring the contribution of a few men of genius, -- and genius is largely independent of the times, --there is not much evidence of such creative work done by our educated men. I may refer also to more modest forms of creativeness, creativeness such as is evidenced in the daily business of our lives, e.g., in the formation of judgments about our real position in the world. We speak of world movements and have a fair acquaintance with the principles and details of Western life and thought, but we do not always sufficiently realize where we actually stand today and how to apply our bookish principles to our situation in life. We either accept or repeat the judgments passed on us by Western culture, or we impotently resent them but have hardly any estimates of our own, wrung from an inward perception of the realities of our position. In the field of politics, for example, we are only today beginning to realize that we have for long wrongly counted on principles that have application only to countries that are already free and already established and have not had sufficient perception of the dark think they call 'power' which is more real than any logic or political scholarship. In the field of social reform, we have never cared to understand the inwardness of our traditional social structure and to examine how far the sociological principles of the West are universal in their application. We have contented ourselves either with an unthinking conservatism or with an imaginary progressiveness merely imitative of the West.

Then again in the field of learning, how many of us have had distinctively Indian estimates of Western literature and thought? It is possible for a foreigner to appreciate the literature of a country, but it is only to be expected that his mind would react to it differently from the mind of a native of the country. A Frenchman, for example, would not I imagine, appreciate Shakespeare just as an Englishman would do. Our education has largely been imparted to us through English literature. The Indian mind is much further removed by tradition and history than the French or the German mind from the spirit of English literature, and yet no Indian, so far as I am aware, has passed judgments on English literature that reflect his Indian mentality. His judgments do not differ materially from the judgment of an English critic and that raises the suspicion whether it is his judgment at all, whether it is not merely the mechanical thinking of the galvanic mind induced in us through our Western education. In philosophy hardly anything that has been written by a modern educated Indian shows that he has achieved a synthesis of Indian thought with Western thought. There is nothing like a judgment on Western systems from the standpoint of Indian philosophy, and although some appraisement of Indian philosophy has been attempted from the Western standpoint, there appears to be no recognition yet that a criticism of the fundamental notions of either

philosophy is necessary before there can be any useful comparative estimate. And yet it is in philosophy that one could look for an effective contact between Eastern and Western ideas. The most prominent contribution of ancient India to the culture of the world is in the field of philosophy and if the modern Indian mind is to philosophize at all to any purpose, it has to confront Eastern thought and Western thought with one another and attempt a synthesis or a reasoned rejection of either, if that were possible. It is in philosophy, if anywhere, that the task of discovering the soul of India is imperative for the modern Indian: the task of achieving, if possible, the continuity of his old self with his present-day self, of realizing what is nowadays called the Mission of India, if it has any. Genius can unveil the soul of India in art, but it is through philosophy that we can methodically attempt to discover it. Our education has not so far helped us to understand ourselves, to understand the significance of our past, the realities of our present and our mission of the future. It has tended to drive our real mind into the unconscious and to replace it by a shadow mind that has no roots in our past and in our real present. Our old mind cannot be wholly driven underground and its imposed substitute cannot function effectively and productively. The result is that there is a confusion between the two minds and a hopeless Babel in the world of ideas. Our thought is hybrid through and through and inevitably sterile. Slavery has entered into our very soul.

The hybridization of our ideas is evidenced by the strange medley of vernacular and English in which our educated people speak to one another. For the expression of cultural ideas specially we find it very difficult to use the pure vernacular medium. If I were asked, for example, to conduct today's discourse here in Bengali, I would have to make a particularly strenuous effort. One notices a laudable tendency at the present day to make such an effort. It is not that it is always successful. Perhaps that is only to be expected in a period of transition. If the language difficulty could be surmounted, it would mean a big step towards the achievement of what I have called Swaraj in Ideas. The hybridization of ideas brought about by our education and the impact of Western political, social and economic institutions of our daily life is one of the most distressing features of our present situation. It is unnatural and may be regarded with the same sentiment with which an old world Hindu looks upon varna-samkara. It does not simply mean a confusion in the intellectual region. All vital ideas involve ideals. They embody an entire theory and an insight into life. Thought or reason may be universal, but ideas are carved out of it differently by different cultures according to their respective genius. No idea of one cultural language can exactly be translated in another cultural language. Every culture has its distinctive 'physiognomy' which is reflected in each vital idea and ideal presented by the culture. A patchwork of ideas of different cultures offends against scholarly sense just as much as patchwork of ideals offends against the spiritual sense. There is room indeed for an adjustment and synthesis, within limits of different cultures and cultural ideals. Life means adaptation to varying times and to varying ideals. But we are not always clear about the method of this adaptation. As we have to live, we have to accept facts and adapt our secular life and secular ideas to the times. We have to alter ourselves here to suit the situation. In spiritual life, however, there is no demand for compromising our ideals in order to have a smooth sailing with the times.

Here, if possible and so far as lies in our power, the times have to be adapted to our life and not our life to the times. But the world confronts us not only with aggressive interests but also with aggressive ideals. What response should our traditional ideals make to these imposed ideals? We may respect the new ideals without accepting them, we may attempt a synthesis without compromise or we may accept them as the fulfilment of our ideals. Different responses may be demanded with respect to different ideals, but in any case a patchwork without adjustment or with a mechanical adjustment, if complacently accepted as a solution, is an evil, as no ideal here gets the entire devotion of the soul. Where different ideals are

accepted in the prayerful hope that a synthesis will come, the patchwork is not accepted as a solution and need not be an evil. We talk – a little too glibly perhaps – of a conflict of the ideas and ideals of the West with our traditional ideas and ideals. In many cases it is confusion rather than a conflict and the real problem is to clear up the confusion and to make it develop in the first instance into a definite conflict. The danger is in the complacent acquiescence in the confusion. The realization of a conflict of ideals implies a deepening of the soul. There is conflict proper only when one is really serious about ideals, feels each ideal to be a matter of life and death. We sometimes sentimentally indulge in the thought of a conflict before we are really serious with either ideal. We speak also a little too readily of the demand for a synthesis of the ideals of the East and the West. It is not necessary in every case that a synthesis should be attempted. The ideals of a community spring from its past history and from the soil: they have not necessarily a universal application, and they are not always self-luminous to other communities. There are ideals of the West which we may respect from a distance without recognizing any specific appeal to ourselves. Then again there are ideals that have a partial appeal to us, because they have an affinity with our own ideals, though still with a foreign complexion. What they prescribe to us is to be worshipped in our own fashion with the ceremonials of our own religion. The form of practical life in which an ideal has to be translated, has to be decided by ourselves according to the genius of our own community. A synthesis of our ideal with western ideals is not demanded in every case. Where it is demanded, the foreign ideal is to be assimilated to our ideal and not the other way. There is no demand for the surrender of our individuality in any case: Svadharme nidhanam sreyah paradharmo bhayaavahah. There are those who take this emphasis on the individuality of a historical community to be overstrained. It appears to them to be the expression of national, communal or racial conceit and the excuse for a perverse obscurantism. They believe in abstract self-luminous ideals for all humanity, in a single universal religion and a single universal region.

There is, however, a case for universalism. The progress of a community and of humanity implies a gradual simplification and unification of ideals. This is just the rationalizing movement, the emergence of a common reason. We have to distinguish, however, between two forms of rationalism, two directions of this simplifying movement. In the one, reason is born after the travail of the spirit: rationalism is here the efflux of reverence, reverence for the traditional institutions through which customary sentiments are deepened into transparent ideals. In the other form of rationalism – what is commonly meant by the name, the simplification and generalization of ideals is effected by unregenerate understanding with its mechanical separation of the essential from the inessential. The essential is judged as such here not through reverence, not through deepened spiritual insight, but through the accidental likes and dislikes of the person judging. Customs and institutions bound up with age-long sentiments are brushed aside (in the name of reason) as meaningless and dead without any imaginative effort to realize them in an attitude of humility. Decisions as to what is essential or inessential have indeed to be taken, for time tarries not and mere historical sentimentalism will not avail. In practical life, one may have to move before ideals have clarified; but it is well to recognize the need of humility and patience in the adjustment of the world of ideas. Order is evolved in the world of our ideas through infinite patience and humility. That is the right kind of rationalism: it is only in the wrong and graceless form of rationalism that brusque decisions in the practical manner are taken in the name of reason, in the world of our ideals. There is then a legitimate and obligatory form of rationalism. It is wrong not to accept and ideal that is felt to be a simpler and deeper expression of our own ideals simple because it hails from a foreign country. To reject it would be insist on individuality for the sake of individuality and would be a form of national conceit and obscurantism. The acceptance of

such an ideal is really no surrender of individuality: to serve this foreign god is to serve our own god: the foreign ideal is here in our own ideal. The guru or teacher has to be accepted when he is found to be a real guru, whatever the community from which he comes. But it is not every foreign ideal that is felt to be the should of our own ideal. Some foreign ideals have affinity with our own, and are really alternative expressions of them in a foreign idiom that has not sacredness for us and there are others which have no real application to our conditions.

It is sometimes forgotten by the advocates of universalism that the so-called universalism of reason or of religion is only in the making and cannot be appealed to as an actually established code of universal principles. What is universal is only the spirit, the loyalty to our own ideals and the openness to other ideals, the determination not to reject them if they are found within our ideals and not to accept them till they are so found. The only way to appraise a new ideal is to view it through our actual ideal; the only way to find a new reverence is to deepen our old reverence. Progress in the spiritual world is not achieved by a detached reason judging between an old god and a new god. The way to know facts is not the way to know values. So much for the objection, which is often raised in the name of universalism, to the stress I have laid on the individuality of Indian thought and spirit, on the conservatism of the distinctive values evolved through ages of continuous historical life of Indian society. I have thought it necessary to examine universalism in some detail at the risk of tiring the reader with abstract arguments because this appears to me to be our greatest danger. It is the inevitable result of our 'rootless' education and it stands more than anything else in the way of what I call Swaraj in Ideas. The other danger of national conceit and the unthinking glorification of everything in our culture and depreciation of everything in other cultures appears to me, in our circumstances, to require less stressing. Not that it is less serious abstractly considered, but as a matter of fact our educated men suffer more from over-diffidence than from over-confidence, more from a 'rootless' universalism than from clinging particularism. We are more ready to accept others' judgments about us than to resent them. There is the old immemorial habit of regarding what we are taught as sacred learning, and the habit is not easily altered even though the learning imparted is the mere opinion of others – opinion about us, for example, of men who might be presumed to be ignorant of us and unsympathetic to us. There is so much, kind or unkind, written about us and preached to us by others that raises the legitimate question if they have a sufficient perception of the inwardness of our life. Prima facie it is very difficult for a foreigner to understand the mind of a people from whom he is widely removed by tradition and history unless he has intimately participated in their life for a long time. It is only natural that the people in question should receive his judgment about them with a certain amount of mental reserve. It might lead them to self-examination if the foreigner is not obviously ignorant and abusive; but docile acceptance is not certainly demanded in the first instance.

Now there is a good deal in the name of learning – history, philosophy or moral sermon – imparted to us through our education which is unconsciously or consciously of a tendentious or propagandist character. That imply a valuation of ourselves, an appraisement of our past history and present position from a foreign standard. Our attitude towards them should be one of critical reserve, and not of docile acceptance. And yet the critical attitude would in many cases be condemned by our foreign teachers and by our own educated men as uncultured and almost absurdly ignorant as a hesitation to accept the truth of geometry. That is inevitable where the education of a people is undertaken by foreign rulers. There is bound in such a case to be some imposition of foreign valuations on the learner and a discouragement of the critical attitude. The question of imposition does not arise in the case of certain branches of learning – mathematics and the natural sciences, for example, which have no nationality and

imply no\ valuation. Whenever there is valuation, there is the suspicion of a particular point of view – national, communal or racial, of the person who judges the value. A valuation of our culture by a foreigner from the standpoint of his own culture should be regarded by us as meant not for our immediate acceptance but for our critical examination. It should be a fillip to which we should react. I remember a remark of Sir John Woodroffe to this purpose. That our first impulse here should be one of self-defensive resentment is only natural and need not imply an uncultured self-conceit. Docile acceptance without criticism would mean slavery. The critical attitude is demanded pre-eminently in the field of valuations of ideals. Mere acceptance here makes not only for confusion but for moral evil. But barring the concepts of the sciences – even here there may be some doubt – all concepts and ideas have the distinctive character of the particular culture to which they belong. What should be our reaction to such cultural ideas? They have to be accepted, but as metaphors and symbols to be translated into our own indigenous concepts. The ideas embodied in a foreign language are properly understood only when we can express them in our own way. I plead for a genuine translation of foreign ideas into our native ideas before we accept or reject them. Let us everywhere resolutely think in our own concepts. It is only thus that we can think productively on our own account. In politics our educated men have been compelled to realize by the logic of facts that they have absolutely no power for good, though they have much power for evil, unless they can carry the masses with them. In other fields there is not such realization of this circumstance. In the social sphere, for example, they still believe that they can impose certain reforms on the masses – by mere preaching from without, by passing resolutions in social conferences and by legislation. In the sphere of ideas, there is hardly yet any realization that we can think effectively only when we think in terms of the indigenous ideas that pulsate in the life and mind of the masses. We condemn the caste system of our country, but we ignore the fact that we who have received Western education constitute a caste more exclusive and intolerant than any of the traditional castes. Let us resolutely break down the barriers of this new caste, let us come back to the cultural stratum ofthe real Indian people and evolve a culture along with them suited to the time and to our native genius. That would be to achieve Swaraj in Ideas.

APPENDIX – B

DEFENCE PLANNING COMMITTEE (DPC)

There is no official document so far been released by the Government on DPC. The version of the news report that appeared on 19 April 2018 in HINDUSTAN TIMES is appended below

HINDUSTAN TIMES

https://www.hindustantimes.com/india-news/india-to-create-super-committee-for-defence-planning/story-PQSPeTpZ8Xm2QKjINXzxnK.html

Sisir Gupta 19 Apr 18

India to create super-committee for defence planning

The DPC will be a permanent body chaired by the National Security Advisor and comprise the chairman of the Chiefs of Staff Committee, three service chiefs, the defence, expenditure and foreign secretaries.

india Updated: Apr 19, 2018 07:15 IST

The Narendra Modi government has decided to create an overarching Defence Planning Committee (DPC) under National Security Advisor Ajit Doval that will drive the country's military and security strategy, draft capability development plans and guide (and accelerate) defence equipment acquisitions, according to a defence ministry notification seen by Hindustan Times.

The move, which is a significant change in India's defence strategy architecture, comes as the country faces several potential threats in a highly militarised neighbourhood; is trying to balance budgetary constraints with its need for arms; and is working on increasing its own expertise in manufacturing and exporting defence equipment. Until now, defence planning has been synonymous with hardware acquisition.

The DPC will be a permanent body chaired by the National Security Advisor and comprise the chairman of the Chiefs of Staff Committee, three service chiefs, the defence, expenditure and foreign secretaries, and prepare draft reports on "national security strategy, international defence engagement strategy, roadmap to build (a) defence manufacturing ecosystem, strategy to boost defence exports, and priority capability development plans", according to the notification. It will submit its reports to defence minister Nirmala Sitharaman. The DPC is expected to meet soon after Doval returns from Germany on April 21.

Analysts point out that because the Prime Minister's Office, the defence ministry, the finance ministry and the three services are part of the same committee, decisions on military purchases could now happen much faster.

The Chief of Integrated Defence Staff to the Chairman of the Chief of the Staff Committee (CISC) will be the member secretary of the committee, according to the notification, and the HQ of the Integrated Defence Staff will be the secretariat of the DPC.

The notification lists four sub-committees that could be created under the DPC across four broad areas: policy and strategy; plans and capability development; defence diplomacy; and defence manufacturing eco-system.

While India does have a defence planning architecture in place, this is the first time it is creating a body that will factor in everything from foreign policy imperatives to operational directives and long-term defence equipment acquisition and infrastructure development plans to technological developments in other parts of the world while coming up with a plan.

The DPC will prepare military doctrines and, in turn, define Indian military objectives for the future. The doctrines will reflect India's no-first-use nuclear policy as well as take into account the possibility of a two-front war (on the country's western and northern fronts). They will justify the Indian Navy's demand of two aircraft carriers and the role of Indian Air Force in the era of long range stand-off weapons and missile theatre defence.

Senior defence ministry officials said that defence minister's operational directives will flow out of new military doctrines to ensure that India's strategic interests are not threatened by any of its neighbours, or a proxy. The operational directives are classified instructions issued to any military arm to protect national interest.

DEFENCE PLANNING COMMITTEE: THE CONTOURS

Mandate for sub-committees

1 Policy and Strategy

a. Assess external security risks, define defence and security priorities
b. Formulate and review military and national security strategy

2 Planning & capability development

a. Identify how different ministries can come together for national security issues
b. Create a capability development plan (CDP) and monitor its timely implementation
c. Obtain Cabinet approval and help secure budgetary support

3 Defence diplomacy

a. Evaluate foreign policy needs and create a defence engagement strategy
b. Identify foreign acquisitions and sales to achieve strategic leverage

4 Defence manufacturing

a. Draft comprehensive policy for research and development
b. Draw out road map for indigenization
c. Formulate policy, institute structural framework to boost defence exports

APPENDIX -C

National Cyber Security Policy -2013

Preamble

1. Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

3. Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fueling India's economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India's image to that of a global player in providing world-class technology solutions and IT business services. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc.) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

1ISO / IEC 27032-2012

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services

by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hacktivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified under a National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

III. Objectives

1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.

5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialization leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalize 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.

4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritization, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.

6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research &

Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.
3) To facilitate transition, diffusion and commercialization of the outputs of Research & Development into commercial products and services for use in public and private sectors.
4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.
5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.
I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalization of the Policy

This policy shall be operationalized by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

APPENDIX –D

Draft Defence Production Policy 2018-

Invite for Comments

Govt of India has announced in the General Budget 2018-19 that the Govt will bring out an industry friendly Defence Production Policy 2018 to promote domestic production by public sector, private sector and MSMEs. In pursuance of the above, the Govt. has formulated a draft Defence Production Policy 2018 which is placed below.
It is requested to provide your comments on the draft policy at dirpnc-ddp@nic.in latest by 30.03.2018.

DRAFT
DEFENCE PRODUCTION POLICY 2018

1. Preamble

1.1 Self-reliance in defence production has been the goal of India's defence production strategy since 1960s. Government has also announced a Defence production Policy 2011. Significant progress in domestic defence production has been made. India defence production has progressively increased from Rs. 43,746 crores in 2013-14 to Rs. 55,894 crores in 2016-17. Defence PSUs like HAL in aero, MDL, GRSE, GSL and HSL in naval, BDL, BEML, MIDHANI and OFBs in land systems and BEL in electronics have emerged as significant players in the defence production ecosystem in the country. Several platforms like Air Defence Missile System 'Akash', Light Combat Aircraft 'Tejas', Main Battle Tank 'Arjun', Ballistic Missiles like 'Prithvi', 'Agni', Multi Rocket Launcher System 'Pinaka', Central Acquisition Radar have been designed and produced indigenously and several others like Fighter Aircraft Sukhoi Su-30 MKI & T-90 Tank have been produced based on transfer of technology. However, it is also true that despite some salient achievements of our defence production ecosystem, a significant part of our defence requirements continue to be dependent on imports. India has become one of the largest importer of defence goods and services in the world. This needs to change.

1.2 A vibrant defence industry is a crucial component of effective defence capability, and to achieve national sovereignty and military superiority. The attainment of the same shall ensure:

1.3 R&D and innovation are important determinants of defence production capabilities. The technology change in the information arena, the biological arena and the nano-technology arena is not only going to have a profound impact on military operations, but will also require a much more responsive defence industry, especially in light of the decreasing predictability of future needs. DRDO has 52 labs across all domains of defence for R&D in defence related requirements and has played an important part in new technology

1.2.1 Strategic independence

1.2.2 Sovereign capability in selected areas

1.2.3 Cost effective defence equipment

1.2.4 Collateral benefits ensuing from the endeavors of the defence industry

development in the country. However, we continue to manufacture several technological platforms under licensed-production. World over defence has been a major reason and determinant of technological growth and development. We need to develop cutting-edge technologies to be able to achieve leadership in defence products.

1.4 India has emerged as a top destination for R&D Centres in the world, ahead of US China in 2015 and the trend continues. The R&D strength of India needs to be channelized for creating domestic IPR for defence needs. With the launch of Start-Up India program, India has also become the hotspot of start-up activity in the world, having the third-largest start-up ecosystem globally. These strengths need to be leveraged to catapult India as a developer of next level of frontier defence technologies in the world.

1.5 New and emerging technologies like Artificial Intelligence and Robotics are arguably the most important determinants of defensive and offensive capabilities for any defence force in the future. Most leading countries are working frantically to achieve leadership in these technologies. Cyber space has opened the fourth domain of warfare, beyond Army, Navy and Air force. India, with its leadership in IT domain needs to use this technology tilt to its advantage.

1.6 Government has as part of its 'Make in India' programme has given a new impetus to development of defence production in the country both for its need and also for exporting to friendly countries. Several initiatives have been taken in the last three years to promote greater participation of industry. These include revision in Defence Procurement Procedures to introduce 'Make-I' and 'Make-II' processes, introduction of Strategic Partnership Model, increase in FDI through automatic route to 49%, restricting licensing requirements for critical items, denotifying several items previously produced only by OFBs for production by industry etc.

1.7 Defence Production Policy 2018 attempts to further build on these initiatives and provides a focussed, structured and significant thrust to development of defence design and production capabilities in the country.

2. Vision

To make India among the top five countries of the world in Aerospace and Defence industries, with active participation of public and private sector, fulfilling the objective of self-reliance as well as demand of other friendly countries.

3. Goals and Objectives

The policy has the following goals and objectives:
3.1 Create an environment that encourages a dynamic, robust and competitive defence industry as an important part of the 'Make in India' initiative.
3.2 To facilitate faster absorption of technology and create a tiered defence industrial ecosystem in the country.
3.3 To reduce current dependence on imports and to achieve self-reliance in development and manufacture of following weapon systems/platforms latest by 2025:-
3.3.1 Fighter Aircraft.
3.3.2 Medium Lift and Utility Helicopters.
3.3.3 Warships.
3.3.4 Land Combat Vehicles.
3.3.5 Autonomous Weapon Systems.
3.3.6 Missile Systems.
3.3.7 Gun systems.
3.3.8 Small Arms.
3.3.9 Ammunition and Explosives.
3.3.10 Surveillance Systems.
3.3.11 Electronic Warfare (EW) Systems.
3.3.12 Communication Systems.
3.3.13 Night Fighting Enablers.

3.4 To achieve a turnover of Rs 1,70,000 Crores (USD 26 Bn approx) in defence goods and services by 2025 involving additional investment of nearly Rs70,000 Crores (USD 10 Bn approx) creating employment for nearly 2 to 3 Million people.
3.5 To achieve export of Rs 35,000 Crores (USD 05 Bn approx) in defence goods and services by 2025.
3.6 To make India as a global leader in Cyberspace and AI technologies.

4. Strategies

The Policy is centered on following pillars:
4.1 Fostering a competitive, innovative and robust defence industry.
4.2 Encouraging collaborations to acquire latest technology, manufacturing processes, skill-sets and R&D.
4.3 Providing a boost to MSMEs and Start-ups.
4.4 Strengthening infrastructure, including QA/QC/testing labs, both within public and private sector.
4.5 Enabling ease of doing business.
4.6 Enhancing defence exports.

5. Ease of Doing Business in Defence Production

5.1 To make it easier to do business with defence, particularly for innovators, small and medium-sized enterprises and non-traditional defence suppliers, the following is proposed:
5.1.1 Necessary enabling provisions will be brought in to enable Startups and MSMEs to participate in transparent and fair manner, without having restrictions of turnover, prior experience as they meet technical and functional requirements.

5.1.2 The stipulation that the value-addition for IDDM should be done by one unit will be done away with. The IDDM requirements of value-addition can be met if said value-addition is done within India by multiple units within India. This will enable Startups and MSMEs working in part of the value-chain.

5.2 Undertake 'Competency Mapping' of private defence industry including MSMEs, to establish their core competence/ability to absorb various technologies. Towards this, a new Portal will be opened shortly on DDP website to improve engagement with industry and to facilitate collection/updation of requisite inputs directly from the Indian industry/suppliers. The Portal will also be used to flag new procurement opportunities, as well as explaining new policies and processes.
5.3 Defence Investor Cell in Department of Defence Production will provide handholding to MSMEs and other investor in defence production, as also to resolve issues with Central, State and other authorities.
5.4 Technology Perspective Capability Roadmap (TPCR), which lists out the platform/weapon systems being considered for procurement in the next 10 year timeframe by our Services will also be hosted on Department of Defence Production website to provide our private industry greater visibility into the likely opportunities in the defence sector. Understanding future capital priorities will allow industry to position themselves in an optimal manner to compete at the appropriate time.
5.5 The Simplified Make-II process of DPP 2016 will be streamlined to make it easier for industry to enter in defence production sector.
5.6 Simplified Make-II process provides for proactive suggestions from industry for consideration by services. Services would be encouraged to consider such proposals received from industry.
5.7 Sample survey shall be carried out involving industry units in defence clusters to identify bottlenecks in doing business in defence. Policies will be streamlined based on these feedbacks.

6. Licensing Process

6.1 Licensing process for defence industries will be liberalized. The list of items requiring licenses will be reviewed and pruned. Except a small negative list, other items will be taken out of purview of licensing.

6.2 All applications for licenses will be disposed off in 30 days. NOCs/Comments from all agencies must necessarily be received within two weeks.

6.3 Favorable consideration will be given to the track record of companies for purpose of renewal or additional license.

7. The practice of ex-ante capacity assessment of industrial units will be done away with, in general. Suitable safeguards will be ensured in the RFP through EMDs and performance Guarantees. Only in exceptional cases, involving big value of extremely critical projects, ex-ante capacity assessment will be undertaken.

8. Open Competition

8.1 Open competition, besides maximizing returns on money, is the greatest driver for innovation and productivity, and therefore will remain at the core of defence procurement.

8.2 Revenue procurement and outsourcing of services will be progressively made competitive through increased participation of industry.

8.3 Only niche/core products will be manufactured by OFB. Several non-core items have already been de-notified from the OFB list and Ordnance Factories are competing with industry for supply of these items. This list of items will be progressively reviewed.

9. FDI

9.1 FDI regime in defence will be further liberalized.

9.2 FDI up to 74% under automatic route will be allowed in niche technology areas.

10. Offsets

10.1 New investment linked avenues for discharge of offset obligations will be made available which will also enable certainty and quick discharge of offsets.

10.2 The end-to-end offset process will be made digital to ensure speedy, transparent and efficient management of offset obligations.

10.3 Offsets Ombudsman will be set up to resolve issues arising from claims of offset in a fair, speedy and transparent manner.

11. Tax

11.1 Tax regime will be rationalised to make domestic manufacturing attractive by ensuring there is no tax inversion.
11.2 Taxes on import of capital goods and services, inputs and components used in defence production will be rationalised in this regard.

12. Market Creation

12.1 Aggregation of demand over medium to long term will be the accepted broad policy for attracting investment in major defence production areas. Aggregation of such demand will help attract greater investment interest and reduce prices of identified goods and services. Wherever feasible, aggregation of such demand will also be done across non-defence sectors including the needs of internal security, civil aviation sector, shipping sectors etc.
12.2 Wherever applicable, life time support for large platform will be included while inviting bidders to set up production facility. This will enable setting up adequate facilities for spare, repair and maintenance during the life-cycle of the platform.

13. Vendor Development and Outsourcing

13.1 OFB and DPSUs will focus on system integration, design and development, and will actively engage domestic vendors in the private sector for other assembly work.

13.2 Similarly, private defence majors will also be encouraged to play the role of a System Integrator and setup an extensive eco-system comprising development partners, specialised vendors and suppliers, particularly from the MSME sector.

14. Infrastructure Development

Success of the policy is dependent upon a genuine partnership with industry, which helps to build a robust defence eco-system and creates jobs across the country. Towards this, following steps are envisaged:
14.1 Defence Industry Corridors: Two Defence industry Corridors will be set up in collaboration with States to provide state-of-the-art infrastructure and facilities for setting up defence production facilities.
14.1.1 These Defence Corridors will be built on existing defence production facilities and will set up new industry clusters to create a synergistic

supply chain of MSMEs and OEMs with necessary testing and certification facilities, export facilitation centres, technology transfer facilitation etc.
14.1.2 Govt of India will contribute 50% of assistance subject to a ceiling of Rs 3000 Crores to the SPV set up for development of each defence corridor. The SPV will take up projects for creating necessary eco-system for defence production in these corridors.

14.1.3 In each Defence Corridor, one major cluster of defence production units around an anchor unit will be developed in one of the Nodes of the Defence Corridor.
14.2 Testing Infrastructure
14.2.1 The existing with Defence organizations will be made available for private industry use.
14.2.2 Government will also set up testing facilities for industry use, and/or
14.2.3 Create a scheme for providing 75% assistance to industry to set up common testing facilities subject to a ceiling of Rs 100 crores per facility. Detailed scheme will be notified later.

15. Boosting OFB and Public Sector

15.1 Government will support infusion of new technology/machineries in OFB/DPSUs to enable them take up advanced manufacturing/development of futuristic weapons and equipment.
15.2 OFB/DPSUs will be encouraged to increase productivity and timely execution of orders by addressing issues of high inventory handling, greater vendor outsourcing, improving skill levels, overall program management etc. Greater use of IT based systems including systems for supply chain management customer relationship management, data analytics, etc, will be adopted.
15.3 Ordnance Factories will be professionalized to make them competitive and improve their productivity.

15.4 Disinvestment of minority stake in DPSUs will be pursued.
15.5 DPSUs/OFB will explore acquisition of technology through mergers/acquisitions globally.
15.6 Cyber security framework will be put in place for DPSUs and OFBs to prepare them for leveraging capabilities of cyber space in their respective functions.

16. Standardization and Quality Assurance

16.1 The quality control process will be reviewed and aligned with the best global practices.
16.2 Simulation based testing will be encouraged and greater emphasis will be laid on acceptance of certification from accredited laboratories. Towards this, DGQA will promulgate a detailed list of environmental tests, which are supportable by certification/simulation, for reference of industry.
16.3 Third-party and self-certification will be promoted across all platforms and throughout value chain.
16.4 Pool of test beds/firing ranges/QA-QC labs will be mapped in the country and wherever required new QA/QC and testing facilities/labs will be setup both in the Govt departments as also the private sector.

17. Export Promotion

17.1 Defence Expo and Aero Expo will be positioned as major global events to showcase India's capabilities in defence manufacturing, as also to encourage exports.
17.2 Subject to strategic considerations, domestically manufactured defence products of both public sector organizations and private industry will be promoted through Govt to Govt agreements and Line of Credit/Funding.

17.3 Indian Offset Partners will be encouraged to take up export of parts and accessories developed as part of offset process.
17.4 DPSUs/OFBs will set up export offices in countries having such potential with the objective of promoting exports actively.

17.5 Defence Export Organization will be set up jointly with industry to promote export of Indian defence products abroad.
17.6 The end-to-end export clearance process in the Department of Defence Production will be made online and time-bound.

18. Innovation and R&D

18.1 While promoting the public sector based R&D ecosystem developed through DRDO labs, efforts will be to create an active and healthy innovation and R&D ecosystem for Defence technologies in partnership with the industry.
18.2 A High Level mechanism with involvement of Service organizations and HQIDS will be set up for identifying capability voids and defining critical technologies required for indigenous research/manufacturing in consultation with industry and academia. They will provide advice regarding technology platforms, which should be developed in the country in the medium and long term. Wherever required, Government will provide support for development of such platforms.
18.3 R&D capability mapping will be done to identify defence related technologies. This mapping will cover DRDO labs, other public sector laboratories, academic institutions and industry.
18.4 Support will be given for speedily indigenizing components/sub-assemblies from foreign OEMs, which are used for manufacture of final products under licensed production in the country.
18.5 Services/DPSUs/OFs have worked out formal arrangements for research with top end technical institutions in the country. This initiative will be encouraged and will be further spread to other academia/higher learning institutions to spur R & D in select fields as well as to build indigenous capacities to undertake substantial technology upgrades.
18.6 Centres of Excellence with industry participation and with Government support, will be set up in niche areas to enable development of frontier technology areas with active involvement of academia and R&D institutions.
18.7 Competitive funded prototyping will be pursued during the design process to address the multiple challenges of technical feasibility, affordability, producibility and supportability.

19. Start-ups

19.1 Start-ups will be involved in the technology development in aerospace and defence sectors.
19.2 Hackathons will be conducted on specific problem areas. Department of Defence Production and DRDO will announce challenges for major defence R&D requirements for institutions to participate with well-defined outcomes. An amount of Rs 1000 crores will be allocated for this purpose for period 2018-2022.
19.3 A scheme entitled Innovation for Defence Excellence (iDeX) will be formulated which will set up Defence Innovation Hubs throughout the country to provide necessary incubation and infrastructure support to the start-ups in defence area. Wherever required, private venture capital into the defence sector, especially for start-ups will be encouraged.

19.4 Government will come up with appropriate policy for Start-ups in strategic areas to monetize the newly developed technologies. The policy will, inter-alia, provide Right of First Offer to Government to acquire the technology through appropriate market based acquisition process.
19.5 An Intellectual Property Cell will be set up in Department of Defence Production for promoting creation of Intellectual property in the sector. The Cell will, inter-alia, provide legal and technical assistance for identifying and registering intellectual property in aerospace and defence related sectors.
19.6 Priority will be given to registration of intellectual property involving national security and defence and aerospace related technologies.

20. Aerospace

20.1 DDP will consult all stakeholders and explore possibility of a setting up an autonomous National Aeronautical Commission, in line with Nuclear or Space Commissions tobring focus onto following important areas:
20.1.1 Leverage mutually beneficial links between military and civil aviation for expansion and, importantly, indigenization.
20.1.2 Bring together diverse agencies for synergies in technology development, basic and fundamental research and production.
20.1.3 Create a scenario in which the benefits of a competitive environment are felt in all areas of the economy as a whole and the defence economy in particular.
20.2 An Aeronautical University will be set up as an autonomous institution to promote design, development and manufacturing industry in the country on a 50:50 cost-sharing basis between Government and HAL.
20.3 Automotive component manufacturers and other similarly relevant industries will be encouraged, through appropriate skill development and technology upgradation initiatives, to transition to aerospace component design and manufacturing.
20.4 Financial and fiscal incentives will be provided for promoting MRO in aerospace sector.
20.5 Leveraging the design and manufacturing capabilities developed in the country for developing various flying platforms, Government will develop civilian aircraft of 80 to 100 seats over the next 7 years.
20.6 Capacities to produce various platforms, including Light Combat Aircraft (LCA), Advance Light Helicopter (ALH), Light Combat Helicopter (LCH), Light Utility Helicopter (LUH), Dornier 228 will be augmented to meet the requirement of forces as well as export. Appropriate models, including joint offshore manufacturing, will be explored for global market.
20.7 Global majors will be encouraged to set up manufacturing capabilities of their platforms in India, both to cater to domestic needs and export from India.

21. Electronics and Cyber Space

21.1 To leverage India's strength in IT/software area and a program to incentivise development of specific technologies relating to cyberspace will be formulated.
21.2 A Task Force involving experts from Industry, Academia, DRDO, and Government has been set up to chalk out the strategic roadmap for Defence in the area of Artificial Intelligence and Robotics has been set up recently. Necessary mechanism will be set up to implement the recommendations.

21.3 Support will be provided to strengthen cyber security infrastructure for defence related systems in the country.
21.4 Secure communication devices, secure microprocessors and secure mobile phone development will be supported.
21.5 Viability of chip-level fabrication (Silicon, GaN, etc.) will be supported in collaboration with similar efforts being taken up in Ministry of Electronics and IT.

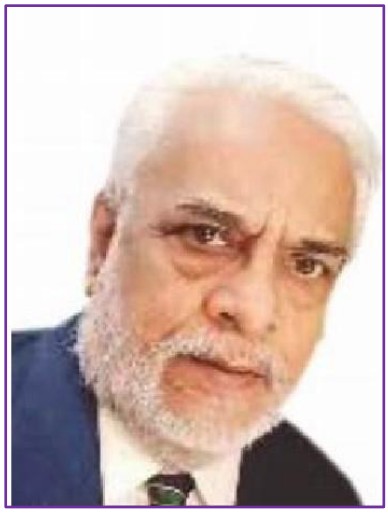
22. Governance

22.1 Department of Defence Production (DDP), Ministry of Defence will be the nodal department for implementation of the Defence Production Policy 2018.
22.2 Legal framework will be put in place to ensure that technology and other sensitive information shared with industry is safeguarded and put in place. Trusted supply chains will be encouraged in defence production ecosystems.
22.3 All AoNs involving domestic production will be reviewed by HQIDS in a time-bound manner and their implementation expedited. Those AoNs where further progress is not likely, will be appropriately closed and necessary steps to issue fresh AoNs initiated.
22.4 Awards and Recognition are currently available for DPSUs and OFBs. DDP will institute similar awards and recognition for well-performing private industry and start-ups.
22.5 As far as possible, all requirements of forces will be manufactured domestically. Where the capability to manufacture does not exist in Indian industry, transfer of technology or enhanced FDI will be considered to enable domestic production. Imports will be resorted only in exceptional situation.
22.6 The Government e-Marketplace (GeM) will be used for those items, which are repeatedly required for needs of the forces and for which adequate supplier base exists.
22.7 State Governments will be encouraged to come up with State specific aerospace and defence related policies to attract investment in this sector. Some states have already taken the initiative in this regard.
22.8 Department of Defence Production will hold regular interactions with all stakeholders, including industry, to foster a partnership model for growth of aerospace and defence sector in the country.
22.9 All stakeholders; DDP, Services, DRDO, DPSUs will conduct regular Outreach Programmes in various parts of the country to interact with industry, especially MSMEs, to spread awareness about the potential opportunities, as also understand the challenges being faced by them. Setting-up of Zonal Liaison/Development Nodes will also be considered.
22.10 Services will also be encouraged to hand-hold defence industry through continuous interaction, sharing of information and arranging visits to repair establishments/field depots for better understanding/appreciation of the requirements.
22.11 Public Procurement Order will be made applicable for procurement of those items in Defence sector for which tenders are global and domestic production capability exists.
22.12 Institutional data collection mechanism regarding Aerospace and Defence industries in the country, including production, export, import, will be put in place.

APPENDIX –E

JOINT DOCTRINE OF INDIAN ARMED FORCES 2017
https://www.ids.nic.in/IDSAdmin/upload_images/doctrine/JointDoctrineIndianArmedForces2017.pdf

The above is a 94 page document and can be accessed in the link given above.



Professor Gautam Sen is concurrently Distinguished Visiting Fellow, Center For Land Warfare Studies, Delhi, Adjunct Professor at National Institute of Advance Studies, Bangalore, Air Marshal Subroto Mukherjee Chair of Excellence, USI, Delhi and the Founder Member and Member Governing Council, Centre for Advance Strategic Studies, Pune ***Professor Sen was formerly*** *Sawarkar Professor of Strategic Studies (1981-2007), Head Department of Defence Studies (1981-2001), Director Post Graduate Studies (1993-2001) Director Board of Colleges & University Development (2001-2004) Founder Director National Centre of International Security and Defence Analysis (NISDA,2002-2007) all at the University of Pune, He was Director General and Member Board of Trustees, Indian Institute of Education, Pune (2006-2011). He has been a Visiting Professor at Madras University, Gujrat Vidyapith, Goa University, Institute of Social and Economic Change, Bangalore and UGC Visiting Professor at Gorakhpur University. Fellow of IISS, London, Jean Monnet Fellow, European University Institute, Florence.* ***Sen lives in Pune, Address: B-304 Twin Towers, Survey No. 164+165, Near Wireless Colony, Aundh, Pune, 411007, Maharashtra; Email: sgautam42@gmail.com; Mob: +91-98-905-92888***

Founded in 2005, Policy Perspectives Foundation (PPF) is a non-profit apolitical think tank. Its activities focus on complex and inter-connected challenges to internal peace, stability and development in India. It promotes debates and dialogues with scholars, development practitioners, civil society, government organisations and other stakeholders, and undertakes training, research and advocacy programmes on issues of national interest.

Policy Perspectives Foundation (PPF) J- 5, First Floor, Green Park Extn., New Delhi-110016